KAJIAN TENTANG KRIPTOSISTEM MCELIECE DALAM MENGHADAPI TANTANGAN KOMPUTER KUANTUM DI ERA REVOLUSI INDUSTRI 4.0

Nur Fadilatul Ilmiyah
Program Studi Tadris Matematika, Institut Agama Islam Negeri Kediri
e-mail: nur.fadilatul.ilmiyah@gmail.com

Received: *Revised:* *Accepted:*

ABSTRAK

Revolusi industri 4.0 ditandai dengan mulai berkembangnya berbagai macam terobosan teknologi baru di bidang robotik, kecerdasan buatan dan komputer kuantum. Komputer kuantum mampu menembus kriptosistem yang mendasarkan keamanannya pada tingkat kesulitan memfaktorkan bilangan bulat integer yang besar. Kriptosistem McElice merupakan kriptosistem kunci publik berbasis teori koding pertama yang dinilai aman untuk diaplikasikan dalam komputer kuantum. Pada konstruksi awalnya kriptosistem ini menggunakan kode Goppa biner tak tereduksi untuk melakukan proses enkripsi dan dekripsi pesan. Artikel ini membahas tentang gambaran umum kriptosistem McEliece meliputi: (1) proses pembentukan matriks *parity-check* dan matriks pembangkit kode Goppa, (2) penentuan dimensi dan jarak minimum kode Goppa biner tak tereduksi, (3) proses *encoding* dan *decoding* pada kode Goppa biner tak tereduksi, (4) aplikasi kode Goppa dalam kriptosistem kunci publik McEliece, serta (5) kelebihan dan kelemahan kriptosistem kunci publik McEliece.

Kata kunci : kode Goppa biner tak tereduksi, kriptosistem berbasis kode, kriptosistem kunci publik, kriptosistem McEliece.

ABSTRACT

The Fourth Industrial Revolution is marked by emerging technology breakthroughs in a number of fields, including robotics, artificial intelligence, and quantum computers. Quantum computers are capable to destroying cryptosystem that based on the difficulty of factoring large integers. The McEliece cryptosystem is the first public key cryptosystem based on coding theory and can be considered as a secure scheme to be implemented in the quantum computer. The early construction of this cryptosystem uses binary irreducible Goppa code to encrypt and decrypt messages. This article will discuss an overview of McEliece cryptosystem which consists of namely: (1) constructing parity-check matrix and generator matrix of Goppa code, (2) determining dimension and minimum distance of binary irreducible Goppa code, (3) encoding and decoding of binary irreducible Goppa code, (4) application of Goppa code in McEliece public key cryptosystem, and (5) the advantages and disadvantages of McEliece public key cryptosystem.

***Keyword**: binary irreducible Goppa code, code based cryptosystem, public key cryptosystem, McEliece cryptosystem.*

PENDAHULUAN

Revolusi industri 4.0 ditandai dengan mulai berkembangnya berbagai macam terobosan baru di bidang robotik, kecerdasan buatan (*artificial intelligence*) dan komputer kuantum. Revolusi industri mengubah cara kerja manusia dari penggunaan manual menjadi otomatisasi atau digitalisasi. Inovasi menjadi kunci eksistensi dari perubahan itu sendiri. Dalam proses transmisi data jarak jauh, penggunaan sistem digital merupakan pilihan yang terbaik. Namun transmisi data yang menjangkau lebih dari ratusan atau ribuan kilometer memungkinkan peluang terjadinya error menjadi semakin besar (Anggraeni,2004). Gangguan-gangguan tersebut menyebabkan pesan yang dikirim tidak sama dengan pesan yang diterima.

Ada berbagai macam kode *error-correcting* yang dapat digunakan untuk memperbaiki kesalahan yang terjadi dalam proses transmisi data, diantaranya adalah kode Hamming. Kode Hamming bekerja dengan memberikan kode biner tambahan pada pesan yang berfungsi sebagai bit-bit pendeteksi kesalahan. Bit-bit ini akan memberikan gambaran mengenai kondisi pesan yang asli. Kesalahan pada pesan yang diterima dapat dideteksi dengan mudah karena terdapat suatu keterkaitan antara pesan dengan bit-bit pendeteksi kesalahan yang dikonstruksikan (Irawanto dan Widyaningsih, 2009).

Permasalahan seputar transmisi data tidak berakhir sampai di sini saja. Setelah teori pengkodean pesan dikembangkan, muncul permasalahan lain berkenaan dengan keamanan proses transmisi pesan yang dikirim melalui komputer atau jaringan internet. Eksistensi internet sebagai media komunikasi umum memungkinkan setiap orang untuk bisa mengaksesnya secara bebas. Akses internet yang bebas akan memperbesar peluang terjadinya penyadap-an pesan oleh pihak yang tak berwenang. Akhirnya dikembangkanlah suatu cabang ilmu lain yang mempelajari tentang teknik pengamanan transmisi pesan yang kemudian dikenal dengan istilah kriptografi.

Dalam kriptografi dikenalkan dua buah algoritma yaitu Algoritma Kriptografi Kunci Rahasia dan Algoritma Kriptografi Kunci Publik. Perbedaan kedua algoritma ini terletak pada jenis dan banyaknya kunci yang digunakan. Algoritma kriptografi kunci rahasia merupakan algoritma yang pertama kali dikembangkan. Algoritma ini hanya menggunakan satu kunci untuk melakukan enkripsi dan dekripsi pesan. Keamanan algoritma ini bergantung pada kerahasiaan kunci. Membocorkan kunci sama artinya dengan memberikan kesempatan kepada pihak tak berwenang untuk melakukan enkripsi dan dekripsi pada pesan yang dirahasiakan. Karena peluang terjadinya kebocoran kunci sangat besar, maka algoritma ini dianggap kurang efisien sehingga para ilmuwan lebih tertarik untuk mengembangkan algoritma kunci publik dibandingkan dengan algoritma kunci rahasia.

Pada dekade terakhir ini banyak sekali teori dalam matematika khususnya teori di dalam aljabar linier dan aljabar abstrak yang dikembangkan dalam bentuk aplikasi maupun integrasi dengan disiplin keilmuan yang lain. Salah satu contoh dari bentuk integrasi aljabar linier dan aljabar abstrak dengan teori koding dan kriptografi adalah dikembangkannya kriptosistem kunci publik McEliece. Kriptografi McEliece merupakan suatu algoritma kriptografi kunci publik berbasis teori koding dengan menggunakan kode Goppa untuk proses enkripsi dan dekripsinya. Alasan mengapa kriptosistem McEliece menjadi pembahasan menarik adalah karena McEliece digadang-gadang sebagai kandidat terbaik untuk keamanan kriptosistem kunci publik *post quantum* (Siim, 20215).

Artikel ini ditulis dengan tujuan untuk mengkaji lebih dalam mengenai konsep dasar, kelebihan serta kelemahan kriptosistem McEliece. Pembahasan dalam artikel ini menggunakan batasan-batasan sebagai berikut:

1) Polinom penyusun kode Goppa yang digunakan adalah polinom tak tereduksi.
2) Lapangan penyusun kode Goppa yang digunakan adalah F_{2^n}.

ANALISIS PEMECAHAN MASALAH

Metode analisis pemecahan masalah yang digunakan penulis dalam artikel ini adalah studi literatur. Pada penulisan awal akan diberikan definisi-definisi dan poin penting yang berhubungan dengan kriptosistem McEliece. Poin penting yang dimaksudkan meliputi uraian mengenai komputer kuantum, lapangan hingga, ring polinom, kode Goppa biner tak tereduksi, kode linier, kriptografi dan sekilas

mengenai sejarah dan perkembangan kriptosistem McEliece.

Komputer Kuantum

Komputer kuantum tidak menggunakan bits melainkan quantum bits atau qubits. Dalam mekanika kuantum, fenomena *superposisi* diartikan sebagai kemampuan suatu partikel untuk berada dalam dua keadaan sekaligus. Fenomena ini dimanfaat-kan dalam sistem kerja komputer kuantum. Jika pada komputer digital hanya dikenal 0 dan 1, maka dalam komputer kuantum selain 0 dan 1 juga dikenal superposisi dari 0 dan 1. Karena komputer kuantum memiliki kemampuan untuk berada di berbagai macam keadaan, maka komputer ini memiliki peluang besar untuk dapat melakukan penghitungan secara simultan dan jauh lebih cepat dari pada komputer digital Saputra, 2009).

Fenomena lain dari mekanika kuantum yang dimanfaatkan dalam kinerja komputer kuantum adalah *entanglement*. Dua atom yang dikenai gaya tertentu dapat berada dalam keadaan *entanglement*. Atom-atom yang terhubung melalui fenomena *entanglement* ini akan tetap terhubung meskipun jaraknya saling berjauhan. Perlakuan pada salah satu atom akan memberikan dampak juga pada atom pasangannya. Hal inilah yang menyebabkan transfer informasi melalui komputer kuantum dapat dilakukan secara instan dan luar biasa cepat (Saputra, 2009).

Perkembangan komputer kuantum harus diimbangi dengan perkembangan kriptosistem yang baik. Di satu sisi, komputer kuantum memberikan manfaat yang besar bagi manusia khususnya dalam penilaian produktivitas kerja dan efisiensi. Namun di sisi yang lain, dampak buruknya juga akan dirasakan jika pemanfaatannya diarahkan untuk hal-hal negatif dan tidak diawasi dengan ketat. Komputer kuantum mampu menembus kriptosistem yang mendasarkan keamanannya pada tingkat kesulitan memfaktorkan bilangan bulat integer yang besar. Oleh karena itu, pada dekade terakhir ini banyak dikembangkan kriptosistem yang tidak mendasarkan keamannya pada algoritma diskrit suatu angka. Kriptosistem McEliece adalah salah satu contohnya.

Lapangan Hingga dan Ring Polinom

Lapangan hingga atau *finite field F* adalah lapangan yang memuat sejumlah hingga elemen. Jumlah elemen di dalam F disebut orde dari F. Contoh lapangan hingga diantaranya adalah Z_p dengan p bilangan prima.

Misalkan diberikan polinom atas F,

$$f(x) = \sum_{i=0}^{t_1} a_i x^i$$

dan

$$h(x) = \sum_{i=0}^{t_2} b_i x^i$$

dengan $t_1 > t_2$. Didefinisikan operasi penjumlahan dan perkaliannya sebagai berikut:

$$f(x) + h(x) = \sum_{i=0}^{t_1} (a_i + b_i) x^i$$

$$f(x)h(x) = \sum_{k=0}^{t_1+t_2} c_k x^k$$

dengan

$$c_k = \sum_{i+j=k, 0\le i\le t_1, 0\le j\le t_2} a_i b_j.$$

Suatu ring yang dibentuk oleh polinom atas F dengan operasi sebagaimana yang didefinisikan di atas disebut dengan ring polinom atas F dan dinotasikan dengan $F[x]$ (Lidl dan Niederreiter, 1986).

Misalkan

$$f(x) = \sum_{i=0}^{t} g_i x^i$$

adalah sebuah polinom atas ring F dan $f(x)$ bukan polinom nol. Koefisien g_t disebut koefisien tertinggi dari $f(x)$, g_0 disebut suku konstan sedang t disebut derajat polinom $f(x)$ yang kemudian dinotasikan dengan $t = \deg(f(x)) = \deg(f)$. Untuk $f = 0$ maka $\deg(0) = -\infty$. Polinom

dengan derajat 0 disebut polinom konstan. Jika koefisien untuk suku berderajat tertinggi dari $f(x)$ adalah 1, maka $f(x)$ disebut polinom monik (Lidl dan Niederreiter, 1986).

Kode Goppa Biner tak Tereduksi

Kriptosistem kunci publik McEliece mempercayakan keamanannya pada penggunaan keluarga kode yang besar yaitu himpunan kode dengan panjang dan dimensi yang sama. Kode ini haruslah bersifat *unpredictable* karena keamanan sistem bergantung pada fakta bahwa pihak ketiga tidak mengetahui algoritma *decoding* yang dapat digunakan dengan cepat, sehingga mereka terpaksa melakukan proses *syndrome decoding* dalam waktu yang sedikit lebih lama (Au, Turner, dan Everson, 2003).

Kode Goppa $\Gamma(L, g)$ merupakan sebuah kode linier (Lidl dan Niederreiter, 1986). Beberapa hal yang menjadi pertimbangan dipilihnya Kode Goppa sebagai pemegang kunci keamanan dalam kriptosistem kunci publik McEliece diantaranya sebagai berikut (Au, Turner, dan Everson, 2003) :

1) Kode Goppa memiliki algoritma *polynomial time decoding* yang cepat.
2) Kode Goppa mudah untuk dibangkitkan tetapi sulit untuk ditebak. Beberapa polinom tak tereduksi atas lapangan hingga F_{2^m} dapat digunakan untuk mengkonstruksi Kode Goppa, akan tetapi matriks generator dari Kode Goppa hampir acak.

Kode Goppa biner tak tereduksi $\Gamma(L, g)$ atas F_2 dengan polinom Goppa $g(x)$ adalah himpunan semua $(c_0, c_1, \dots, c_{n-1}) \in F_2^n$ sedemikian sehingga identitas

$$\sum_{i=0}^{n-1} c_i g(\gamma_i)^{-1} \frac{g(x) - g(\gamma_i)}{x - \gamma_i} = 0$$

terpenuhi di dalam ring polinom $F_{2^m}[x]$.

Pada kasus polinom tak tereduksi $g(x)$, seluruh elemen γ di dalam F_{2^m} memenuhi $g(\gamma) \neq 0$. Oleh karena itu $L = F_{2^m}$ dapat digunakan, sehingga jumlah maksimum elemen di dalam L adalah $n = 2^m + 1$ (Siim, 2015). Kode Goppa biner tak tereduksi memiliki jarak minimum sedikitnya $2t + 1$ sehingga memiliki kapasistas *error-correcting* yang tinggi sampai pada t buah error. Selain itu bentuk matriks *parity-check* dari kode ini sulit dibedakan dengan matriks biner random. Dua keunggulan ini menjadi alasan kuat mengapa kode Goppa biner tak tereduksi cocok digunakan untuk kriptosistem *post quantum*.

Engelbert, Overbeck dan Schmidt dalam (Engelbert, Overbeck, dan Schmidt, 2007) juga mengemukakan beberapa alasan tambahan mengapa kode Goppa biner tak tereduksi menjadi menarik untuk diimplementasikan dalam kriptografi melalui beberapa poin sebagai berikut:

1) Batas minimal untuk jarak minimum kode Goppa biner tak tereduksi mudah untuk dikomputasikan.
2) Pengetahuan yang baik mengenai polinom pembangkit akan memberikan wawasan kepada pemegang sistem untuk bisa menemukan algoritma *error-correction* yang efisien. Sebagai konsekuensinya, algoritma yang efisien untuk koreksi error tidak akan bisa ditemukan jika penyusup tidak mengetahui polinom pembangkitnya.

Kode Linier

Problem dalam proses penyampaian informasi yang sedang marak diteliti saat ini adalah mengenai *encoding* dan *decoding* pesan. Permasalahan muncul karena pada kenyataannya tidak ada jaringan informasi yang ideal yang mampu mengirimkan pesan secara aman tanpa adanya *noise* atau gangguan. Penyampaian informasi dalam hal ini secara lebih spesifik adalah proses mengirimkan pesan yang terdiri dari karakter-karakter alfabet yang jumlahnya terbatas. Oleh karenanya, himpunan karakter alfabet di sini diasumsikan sebagai suatu lapangan hingga (Lidl dan Niederreiter, 1986).

Metode yang dikembangkan untuk menjamin keamanan dalam proses

pengiriman pesan tergantung dari sifat-sifat yang ada pada lapangan hingga. Ide dasar dalam teori koding aljabar adalah untuk mengirimkan informasi tambahan (*redundant information*) bersamaan dengan pesan yang ingin disampaikan, dalam artian dengan suatu cara yang sistematis pesan asli akan dibuat menjadi lebih panjang (Lidl dan Niederreiter, 1986).

Misalkan diasumsikan bahwa karakter dari pesan asli dan pesan yang terkodekan berasal dari lapangan hingga yang sama, F_q. *Encoding* adalah proses mengkodekan satu blok yang terdiri dari k buah karakter $a_1 a_2 \dots a_k, a_i \in F_q$ menjadi n buah karakter kata kode $c_1 c_2 \dots c_n, c_j \in F_q$ dengan $n > k$. k karakter pertama disebut karakter pesan asli dan $n-k$ karakter terakhihr disebut karakter kontrol. *Decoding* adalah proses mengembalikan n buah karakter kata kode menjadi k buah karakter pesan asli (Lidl dan Niederreiter, 1986).

Untuk mempermudah pemahaman, skema *encoding* juga dapat dipresentasikan sebagai berikut (Lidl dan Niederreiter, 1986).

Misalkan H adalah matriks berukuran $(n-k) \times n$ dengan entri-entri di dalam F_q yang berbentuk,

$$H = (A|I_{n-k}),$$

dimana A adalah matriks berukuran $(n-k) \times k$ dan I_{n-k} adalah matriks identitas berorde $n-k$. Karakter kontrol $c_{k+1} \dots c_n$ dapat dihitung dengan persamaan,

$$Hc^T = 0$$

dengan $c = (c_1 \dots c_n)$ adalah kata kode. Persamaan ini disebut persamaan *parity-check*.

Misalkan H adalah matriks berukuran $(n-k) \times n$ dengan rank $n-k$ dan entri-entri di dalam F_q. Himpunan C yang berisi semua vektor $c \in F_q^n$ sedemikian sehingga $Hc^T = 0$ disebut kode linier (n, k) atas F_q. Bilangan n disebut panjang kode sedangkan k disebut dimensi kode. Jika $q = 2$, maka C disebut kode linier. Elemen-elemen di dalam C disebut kata kode (*code word*). Matriks H disebut matriks *parity-check* dari C (Lidl dan Niederreiter, 1986).

Matriks $G = (I_k | -A^T)$ berukuran $k \times n$ disebut matriks pembangun kanonik untuk kode linier (n, k) dengan matriks *parity-check* $H = (A|I_{n-k})$. Dari persamaan $Hc^T = 0$ dan $c = aG$ maka diperoleh relasi antara H dan G sebagai berikut,

$$GH^T = 0.$$

Misalkan t adalah bilangan asli, kode $C \subseteq F_q^n$ disebut kode $t-$*error-correcting* jika untuk suatu $y \in F_q^n$ terdapat paling banyak satu $c \in C$ sedemikian sehingga $d(y, c) \leq t$ (Lidl dan Niederreiter, 1986).

Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, yaitu *kriptos* yang artinya menyembunyikan. Kriptografi adalah ilmu yang mempelajari tentang teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi, seperti integritas data, kerahasiaan data, serta autentikasi data (Mollin, 2003 ; Menezes, Oorschot, dan Vanstone, 1997). Kriptografi menyedi-akan layanan keamanan untuk melindungi informasi atau pesan yang berbentuk digital.

Menurut Menezes, Oorschot dan Vanstone dalam (Mollin, 2003) terdapat empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu:

1) Kerahasiaan, adalah aspek yang digunakan untuk menjaga isi informasi dari siapapun dari pihak-pihak yang tidak memiliki wewenang untuk mengetahui-nya.
2) Integritas data, adalah aspek yang digunakan untuk menjaga data dari perubahan atau manipulasi yang dilakukan secara tidak sah. Bentuk dari manipulasi data antara lain adalah menghapus, menyisipkan dan mensubti-tusikan data lain kedalam data asli.
3) Autentikasi, adalah aspek yang digunakan untuk mengidentifikasi pihak-pihak yang terlibat dalam pengiriman data serta menjamin keaslian data yang meliputi asal-

usulnya, tanggal asal, isi informasi, tanggal pengiriman dan sebagainya.

4) Nirpenyangkalan, adalah aspek yang digunakan untuk mencegah terjadinya penyangkalan terhadap tanggung jawab suatu tindakan pengiriman informasi.

Kriptografi saat ini telah digunakan dalam berbagai macam aplikasi, mulai dari penarikan uang di ATM, penggunaan kartu cerdas (*smart card*), penggunaan kartu kredit, percakapan dengan telepon genggam, password komputer, televisi, transaksi *e-commerce* di internet, gedung-gedung bisnis, sampai pada pengaktifan peluru kendali dan bom nuklir (Munir, 2006).

Dalam dunia kriptografi dikenal beberapa istilah seperti enkripsi, dekripsi, *plaintext*, *ciphertext* dan sebagainya yang akan dijelaskan lebih detil melalui definisi-definisi berikut. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan asli (disebut *plaintext*) menjadi pesan yang tersembunyi dan tidak dapat dibaca (disebut *ciphertext*). Sedangkan dekripsi adalah proses untuk mengubah *ciphertext* menjadi *plaintext* (Schneier, 1996).

Parameter yang digunakan dalam proses enkripsi dan dekripsi disebut kunci. Dalam kriptografi, kunci memegang peranan yang paling penting karena faktor keamanan yang paling mendasar terletak pada kunci yang diberikan. Fungsi matematis yang digunakan saat melakukan enkripsi dan dekripsi disebut dengan algoritma kriptogra-fi atau *cipher*. Algoritma kriptografi modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma melainkan pada kerahasiaan kunci.

Secara umum algoritma kriptografi dibagi menjadi dua jenis yaitu algoritma kunci rahasia dan algoritma kunci publik. Algoritma kunci rahasia adalah algoritma kriptografi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya. Keamanan algoritma konvensional tergantung pada kunci. Contoh Algoritma kriptografi kunci rahasia antara lain, *Subtitution Cipher*, *Transposition Cipher*, *Block Cipher*, *Stream Cipher* dan sebagainya (Namiesyva, 2012).

Salah satu kelemahan yang paling mendasar dari algoritma kriptografi kunci rahasia terletak pada sulitnya menjaga sinkronisasi kunci privat. Untuk menjaga sistem dari serangan maka kunci privat harus sering diganti, dan proses pengambilan persetujuan atau kesepakatan akan suatu kunci privat harus dilakukan secara personal. Lebih jauh lagi, semakin bertambahnya jumlah pengguna maka semakin besar kemungkinan sistem untuk dirusak sehingga sistem tidak terskalakan dengan baik. Kesulitan-kesulitan seperti ini tidak ditemukan di dalam algoritma kriptografi kunci publik (Roering, 2013).

Algoritma kunci publik adalah algoritma kriptografi yang menggunakan dua buah kunci berbeda untuk proses enkripsi dan dekripsinya. Kunci untuk enkripsi dapat diketahui oleh publik sedangkan kunci untuk dekripsi hanya boleh diketahui oleh pihak yang berwenang (Namiesyva, 2012). Contoh dari algoritma kunci publik adalah RSA, ElGamal, McEliece, LUC dan DSA.

Kriptosistem adalah sistem komputer yang didalamnya melibatkan kriptografi. Suatu kriptosistem biasanya memuat tiga algotitma, yaitu algoritma untuk membangkitkan kunci, algoritma untuk proses enkripsi dan algoritma untuk proses dekripsi (Wahyuni, 2010). Kriptanalis merupakan studi untuk menemukan dan mengeksploitasi kelemahan dari kriptosistem tertentu (Roering, 2013).

Kriptosistem McEliece

Pada tahun 1978 Robert J. McEliece memperkenalkan kriptosistem kunci publik pertama yang berbasis kode error-correcting dan mempercayakan keamanannya pada tingkat kesulitan decoding disertai error yang acak (Au, Turner, dan Everson, 2003). Sejak pertama kali dipublikasikan sampai sekarang,

kriptosis-tem kunci publik McEliece dianggap relatif aman, tentunya dengan pemilihan parameter yang tepat. Hal ini menjadikan kriptosistem McEliece sejajar dengan RSA yang pertama kali dipublikasikan pada tahun 1977. Sebagaimana yang diketahui masyarakat umum, RSA merupakan kriptosistem kunci publik yang paling banyak digunakan sampai dengan saat ini. Kepopuleran RSA membuat masyarakat berasumsi bahwa keamanan kriptosistem ini lebih terjamin dan lebih mapan. Namun relasi kriptosistem McEliece dengan teori koding menjadikan tingkat keamanannya juga patut untuk dipertimbangkan (Siim, 2015).

Kriptosistem kunci publik McElice merupakan kriptosistem berbasis teori koding pertama yang dianggap paling sukses. Pada konstruksi awalnya, kriptosis-tem ini menggunakan kode Goppa biner tak tereduksi untuk proses enkripsi dan dekripsi. Kode Goppa biner tak tereduksi ini cocok untuk diaplikasikan dalam kriptografi karena kemampuan *error-correcting*-nya yang tinggi dan kerapatan matriks generatornya yang terbilang baik sehingga sulit membedakannya dengan matriks biner acak (Siim, 2015).

Sebenarnya telah banyak dikonstruksi kriptosistem berbasis teori koding dengan menggunakan kode lain selain kode Goppa, namun satu-persatu dari kriptosistem tersebut mulai ditinggalkan karena terbukti tidak aman dalam menghadapi serangan yang efisien. Sebagai contoh, pada tahun 1986 Niederreiter dalam jurnalnya *Knapsack-type Cryptosystems and Algebraic Coding Theory* mengenalkan skema kriptosistem dengan menggunakan kode *Generalized Reed-Solomon* (GRS). Skema ini sepadan dengan skema McEliece jika kode GRS yang digunakan diganti dengan kode Goppa. Namun pada tahun 1992 Sidelnikov dan Shestakov melalui paper *On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes* menun-jukkan bahwa skema Niederreiter dengan kode GRS terbukti tidak aman (Engelbert, Overbeck, dan Schmidt, 2007). Pada tahun 1994, Sidelnikov mengusulkan penggunaan kode *Reed-Muller* untuk memperoleh ukuran kunci yang lebih kecil dan proses dekripsi yang lebih cepat. Namun Minder dan Shokrollahi pada tahun 2007 berhasil menerobos keamanan kriptosistem yang mengakibatkan kunci rahasia dapat diketahui melalui kunci publiknya (Siim, 2015).

Pada tahun 2005 Berger dan Loidreau mengenalkan konstruksi kriptosistem McElice dengan menggunakan subkode dari kode Reed-Solomon. Namun kriptosistem ini dapat dilumpuhkan oleh Wieschebrink pada tahun 2010. Kode Gabidulin juga pernah diusulkan sebagai pengganti kode Goppa pada tahun 1994, akan tetapi skema ini pun berhasil dibuktikan tidak aman oleh Gibson pada tahun 1996. Janwa dan Morenoin mengusulkan penggunaan kode geometri aljabar pada tahun 1995, namun keamanan skema ini dapat dipatahkan oleh Couvreur, Corbella dan Pellikaan pada tahun 2014 (Siim, 2015).

Kunci dalam kriptosistem McEliece terdiri dari kunci rahasia dan kunci publik. Kunci rahasia menyimpan dekripsi struktur kode linier yang bergantung pada generatornya, sedangkan kunci publik berupa versi yang 'sedikit acak' dari kode yang sama sehingga sulit untuk membedakannya dengan kode linier yang 'benar-benar acak' (Siim, 2015).

HASIL DAN PEMBAHASAN

Gambaran umum kriptosistem McEliece meliputi: proses pembentukan matriks *parity-check* dan matriks pembang-kit kode Goppa, penentuan dimensi dan jarak minimum kode Goppa biner tak tereduksi, proses *encoding*, koreksi error dan *decoding* pada kode Goppa biner tak tereduksi, aplikasi kode Goppa dalam kriptosistem kunci publik McEliece serta kelebihan dan kelemahan kriptosistem McEliece.

Proses pembentukan matriks parity-check dan matriks pembangkit kode Goppa

Matriks *parity-check* untuk kode Goppa merupakan sebuah matriks yang irisan antara ruang nol-nya dan F_q^n akan menghasilkan kode Goppa $\Gamma(L, g)$ (Lidl dan Niederreiter, 1986). Misalkan $g(x)$ adalah Polinom Goppa dan $L = \{\gamma_0, \dots, \gamma_{n-1}\} \subseteq F_{q^m}$ sedemikian sehingga $g(\gamma_i) \neq 0$ dengan $0 \leq i \leq n-1$. Untuk mengkonstruksi matriks generator Kode Goppa, lakukan langkah-langkah sebagai berikut:

a) Konstruksikan matriks *parity-check* H dengan bentuk sebagai berikut:

$$H = \begin{pmatrix} g(\gamma_0)^{-1} & \cdots & g(\gamma_{n-1})^{-1} \\ g(\gamma_0)^{-1}\gamma_0 & \cdots & g(\gamma_{n-1})^{-1}\gamma_{n-1} \\ \vdots & \ddots & \vdots \\ g(\gamma_0)^{-1}\gamma_0^{t-1} & \cdots & g(\gamma_{n-1})^{-1}\gamma_{n-1}^{t-1} \end{pmatrix}$$

atau menggunakan skema persamaan matriks $H = CXY$ (Jochemz, 2002) dengan

$$C_{t\times t} = \begin{pmatrix} g_t & g_{t-1} & g_{t-2} & \cdots & g_1 \\ 0 & g_t & g_{t-1} & \cdots & g_2 \\ 0 & 0 & g_t & \cdots & g_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & g_t \end{pmatrix};$$

$$x_{t\times n} = \begin{pmatrix} \gamma_1^{t-1} & \gamma_2^{t-1} & \cdots & \gamma_n^{t-1} \\ \gamma_1^{t-2} & \gamma_2^{t-2} & \cdots & \gamma_2^{t-2} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1 & \gamma_2 & \cdots & \gamma_n \\ 1 & 1 & \cdots & 1 \end{pmatrix};$$

$$Y_{n\times n} = \begin{pmatrix} h_1 & 0 & 0 & \cdots & 0 \\ 0 & h_2 & 0 & \cdots & 0 \\ 0 & 0 & h_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & h_n \end{pmatrix}.$$

Bentuk matriks *parity-check* dalam skema dua inilah yang akan digunakan pada pembahasan *decoding* dalam artikel ini.

b) Nyatakan setiap entri di dalam matriks H sebagai vektor, sehingga H dapat dipandang sebagai matriks atas F_q yang berdimensi $mt \times n$.

c) Lakukan operasi baris elementer pada H. Akar-akar dari matriks *parity-check* H membangun sebuah ruang vektor V yang merupakan subruang dari F_q^n. Dari persamaan $Hc^T = 0$ diketahui bahwa kode Goppa adalah ruang vektor dual bagi V. Oleh karena itu, matriks pembangkit G untuk kode Goppa dapat diperoleh dengan cara menghitung basis ruang vektor dual dari V melalui persamaan $Hc^T = 0$. Vektor-vektor di dalam ruang nol dari H membentuk ruang baris matriks G, sehingga baris-baris pada matriks G merupakan vektor-vektor basisnya (Lidl dan Niederreiter, 1986). (Engelbert, Overbeck, dan Schmidt, 2007).

Penentuan dimensi dan jarak minimum Kode Goppa biner tak tereduksi

Kode Goppa biner tak tereduksi memiliki dimensi sedikitnya $n - mt$ dengan jarak minimum paling sedikit $2t + 1$ sehingga kode ini bisa mengoreksi sampai dengan t buah error (Lidl dan Niederreiter, 1986). (Jochemz, 2002). (Engelbert, Overbeck, dan Schmidt, 2007). (Siim, 2015).

Proses encoding pada Kode Goppa biner tak tereduksi

Proses *encoding* pada Kode Goppa tidak jauh berbeda dengan proses *encoding* kode yang lain. Proses ini dilakukan dengan cara mengalikan pesan asli m dengan matriks generator Kode Goppa G sehingga diperoleh kata kode c (Jochemsz, 2002),

$$(m_1, \dots, m_k).G = (c_1, \dots, c_n).$$

Proses koreksi error dengan menggunakan kode Goppa biner tak tereduksi

Selanjutnya diberikan algoritma *error-correcting* Kode Goppa biner tak tereduksi berikut yang diambil dari (Qaradaghi dan Abdulrazaq, 2015):

Misalkan $y = (y_1, \dots, y_n)$ adalah pesan yang diterima dengan t buah error. Untuk melakukan proses koreksi error pada y lakukan langkah-langkah berikut:

a) Konstruksi matriks *parity-check* H untuk Kode Goppa $\Gamma(L, g)$.

b) Definisikan sindrom untuk y sebagai berikut:

$$s(x) = \sum_{i=0}^{n-1} \frac{y_i}{x - \gamma_i}.$$

c) Hitung $\sigma(x)$ dengan langkah-langkah sebagai berikut:

(1) Tentukan $h(x)$ dengan menggunakan Algoritma Euclid yang diperluas sedemikian sehingga,

$$s(x)h(x) \equiv 1 \; mod \; g(x),$$

dengan kata lain $h(x) = s^{-1}(x)$.
Jika $h(x) = x$, maka proses selesai. Jika tidak, lanjutkan langkah berikutnya.

(2) Hitung $d(x)$ sedemikian sehingga,

$$d^2(x) \equiv h(x) + x \; mod \; g(x),$$

dengan kata lain

$$d(x) \equiv \sqrt{h(x) + x} \; mod \; g(x).$$

(3) Tentukan $a(x)$ dan $b(x)$ dengan menggunakan Algoritma Euclid yang diperluas sedemikian sehingga,

$$d(x)b(x) \equiv a(x) \; mod \; g(x).$$

(4) Hitung nilai

$$\sigma(x) = a^2(x) + xb^2(x) \; mod \; g(x).$$

d) Tentukan himpunan *error-location*

$$B = \{i | \sigma(\gamma_i) = 0\}.$$

e) Definisikan $e = (e_1, \dots, e_n)$ dengan ketentuan $e_i = 1$ untuk $i \in B$ dan 0 untuk yang lain.

f) Tentukan kata kode c dengan menggunakan formula $c = y - e$.

Proses decoding pada Kode Goppa biner tak tereduksi

Proses *decoding* dilakukan dengan cara melakukan reduksi pada matriks berikut,

$$\left(\begin{array}{c|c} G^T & \begin{matrix} c_1 \\ \vdots \\ c_n \end{matrix} \end{array}\right) \sim \dots \sim \left(\begin{array}{c|c} I_k & \begin{matrix} m_1 \\ \vdots \\ m_k \end{matrix} \\ \hline D & \end{array}\right) .$$

Aplikasi Kode Goppa dalam Kriptosistem McEliece

Pada bagian ini akan dijelaskan bagaimana penerapan kode Goppa dalam kriptosistem McEliece. Skema ini diambil dari (Roering, 2013) dan (Siim, 2015).

Pertama:

Konstruksi sebuah kode Goppa dengan panjang n dan dimensi k dimana n dan k adalah bilangan bulat positif. Kode Goppa dalam hal ini berfungsi sebagai kunci pribadi. Notasikan kode Goppa ini dengan G.

Kedua:

Konstruksi sebuah matriks nonsingular S berukuran $k \times k$ dengan elemen-elemen 0 dan 1. Matriks ini berfungsi sebagai kunci pribadi.

Ketiga:

Konstruksi sebuah matriks permutasi P berukuran $n \times n$. Matriks ini juga berfungsi sebagai kunci pribadi.

Keempat:

Hitung kunci publik yang merupakan hasil dari perkalian matriks-matriks G, P dan S dengan aturan, $G' = SGP$. Dari perhitungan ini diperoleh dua pasang kunci, pertama kunci publik yakni G', kedua, kunci privat yaitu G, P dan S. Matriks G' membangun sebuah kode linier dengan rata-rata dan jarak minimum yang sama dengan kode yang dibangun oleh G. Matriks G' disebut dengan matriks pembangun publik karena keberadaannya dapat diketahui oleh khalayak umum.

Kelima:

Melakukan proses enkripsi pada *plaintext* dengan langkah-langkah berikut:

a) Terjemahkan pesan ke dalam kode ASCII.

b) Bagi pesan ke dalam blok-blok dimana panjang blok sama dengan dimensi kode Goppa. Notasikan blok pesan dengan $m = m_1, m_2, \dots, m_k$.

c) Ambil vektor biner secara acak dengan panjang n dan bobot t. Notasikan vektor ini dengan e.

d) Hitung $x = mG' + e$. Pesan x adalah pesan yang telah dienkripsi.

Keenam:

Kirim *ciphertex*.

Ketujuh:

Setelah *ciphertext* diterima, lakukan proses dekripsi pada *ciphertext* dengan langkah-langkah sebagai berikut:

a) Hitung $x' = xP^{-1}$, dengan P^{-1} adalah invers dari matriks permutasi P. Diperoleh hasil sebagai berikut:

$$\begin{aligned} x' = xP^{-1} &= (mG' + e)P^{-1} \\ &= (mSGP + e)P^{-1} \\ &= mSGPP^{-1} + eP^{-1} \\ &= mSGI + e' \\ &= mSG + e' \end{aligned}$$

b) Aplikasikan algoritma *decoding* pada x' sehingga diperoleh $u = mS$.

c) Kalikan u dengan S^{-1} sehingga diperoleh $m = uS^{-1}$.

Kedelapan:

Gabungkan seluruh blok-blok m kemudian terjemahkan m ke dalam bentuk alfabet biasa sehingga diperoleh pesan asli.

Kelebihan dan Kelemahan Kriptosistem McEliece

Beberapa kelebihan yang dimiliki oleh Kriptosistem McEliece diantaranya adalah sebagai berikut:

1) Sistemnya elegan, mudah dipahami dan keamanannya telah teruji sejak tahun 1978 (Jochemz, 2002).
2) Kriptosistem McEliece memiliki waktu eksekusi yang cepat jika dibandingkan dengan RSA (Siim, 2015).
3) Kriptosistem McEliece dinilai efisien dan aman untuk diaplikasikan dalam komputer kuantum karena beberapa alasan sebagai berikut:

RSA mendasarkan keamanannya pada tingkat kesulitan memfaktorkan bilangan bulat integer yang besar. RSA akan menjadi lemah jika dipraktekkan di dalam komputer kuantum karena dalam komputer kuantum terdapat sebuah algoritma yang dapat memfaktorkan integer secara efisien (Roering, 2013). Sebagaimana RSA, beberapa kriptosistem kunci publik yang terkenal lainnya juga mengandalkan keamannya pada tingkat kesulitan menemukan algoritma diskrit dari suatu angka, tetapi keamanan pada kriptosistem McEliece tidak bergantung pada hal-hal tersebut (Au, Turner, dan Everson, 2003).

a) Kriptosistem McEliece mencoba untuk memasukkan elemen random dalam tiap proses enkripsi guna memperbaiki tingkat keamanan sistem. Elemen random yang dimaksudkan dalam hal ini adalah vektor error e yang dibangkitkan secara acak (Roering, 2013).

Adapun kekurangan yang dimiliki oleh kriptosistem McEliece adalah ukuran kunci publiknya yang terlalu panjang. Ukuran kunci yang besar membuat kriptosistem ini tidak bisa diaplikasikan pada perangkat dengan kapasitas rendah seperti *smartphone* (Jochemz, 2002). Pada tahun 2010, Bernstein mempresentasikan sebuah serangan efisien untuk melumpuhkan kriptosistem McEliece dengan menggunakan algoritma quantum *Grover*. Bernstein menunjukkan bahwa kriptosistem McEliece akan dapat menjaga kemanan post-quantum jika ukuran kuncinya kelipatan empat (*quadrupled*) (Siim, 2015).

SIMPULAN

Kriptosistem McElice dinilai aman untuk diaplikasikan dalam komputer kuantum karena sistem keamanannya tidak bergantung pada algoritma diskrit bilangan, yang mana algoritma ini sangat mudah untuk dipecahkan dalam komputer kuantum. Kelebihan kriptosistem kunci publik McEliece diantaranya: (1) sistemnya elegan, mudah dipahami dan keamanannya telah teruji sejak dari awal dikenalkan, (2) memiliki waktu eksekusi yang cepat, dan (3) efisien untuk diaplikasikan dalam komputer kuantum. Adapun kelemahan dari kriptosistem McEliece ini terletak pada ukuran kunci publiknya yang sangat panjang sehingga kriptosistem ini jarang digunakan.

DAFTAR PUSTAKA

Menezes, A. J., Oorschot, P. C., dan Vanstone, S. A. 1997. *Handbook of Applied Cryptography*, 1st ed. Boca Raton: CRC Press.

Wahyuni, A. Januari, 2010. Aplikasi kriptosistem dengan Algoritma McEliece. *Majalah Ilmiah INFORMATIKA*, vol.1, no.1, pp.1-7.

Irawanto B., dan Widyaningsih, S. 2009. Deteksi dan koreksi error pada pesan digital dengan kode Hamming. *Jurnal Sains dan Matematika*, vol.17, no.3, pp.127-130.

Schneier, B. 1996. *Applied Cryptography, 2nd ed.* New York: John Wiley and Son.

Roering, C. 2013. *Coding Theory Based Cryptography: McEliece Cryptosystem in Sage*. M.S. Honors Theses, Collage of Saint Benedict/ Saint Johns University at Minnesota.

Engelbert, D., Overbeck, R., dan Schmidt, A. 2007. A Summary of McEliece-Type Cryptosystems and their Security. *J. Math. Crypt*, vol.1, pp. 151-199.

Jochemsz, E. 2002. *Goppa Codes and The McEliece Cryptosystem*. Ph.D. Dissertation, University of Amsterdam at Netherland.

Saputra, H. 2009. Kajian tentang komputer kuantum sebagai pengganti komputer konvensional di masa depan. *Jurnal Generic*, vol.4, no.2, pp.15-18.

Mollin, R. A. 2003. *RSA and Public Key Cryptography*, 1st ed., Boca Raton: A CRC Press Company.

Lidl R., dan Niederreiter, H. 1986. *Introduction to finite fields and their applications*, 1st ed., Cambridge: Cambridge University Press.

Munir, R. 2006. *Kriptografi*, 1st ed., Bandung: Penerbit Informatika.

Au, S., Turner, C. E., dan Everson, J. 17 September, 2003. *The McEliece Cryptosystem.*

Siim, S. 28 Mei, 2015. *Study of McEliece Cryptosystem.* Research Seminar in Cryptography, Report in MTAT.07.022.

Qaradaghi T. M., dan Abdulrazaq, N. N. 2015. Comparison between separable and irreducible Goppa code in McEliece Cryptosystem. Q *International Journal Of Computer, Electrical, Automation, Control and Information Engineering*, vol.9, no.10, pp.1975-1981.

Namiesyva. T. 2012. Kriptografi sebagai Media Pembelajaran dalam Studi Matematika Tingkat Sekolah. [Online]. Available: http://informatika.stei.itb.ac.id/~rinaldi.munir/

Anggraeni, W. 2004. Deteksi dan koreksi kesalahan informasi dalam sandi biner dengan menggunakan metode Hamming. *JUTI*, vol.3, n0.2, pp.101-108.