Studi dan Implementasi Algoritma kunci publik McEliece

Widhaprasa Ekamatra Waliprana - 13508080
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18080@students.if.itb.ac.id

***Abstract*—Kriptografi merupakan ilmu dalam menjaga kerahasiaan pesan. Ilmu ini sudah digunakan sejak zaman dahulu. Sampai saat ini ilmu kriptografi semakin digunakan bahkan sampai menjadi kebutuhan sehari-hari. Contoh dari ilmu kriptografi adalah algoritma kunci publik atau algoritma asimetrik. Algoritma kunci publik adalah algoritma pengenkripsian dengan menggunakan kunci publik sebagai media pengenkripsian dan kunci privat sebagai media pendeskripsian. Kunci publik bersifat tidak rahasia, sedangkan kunci privat bersifat rahasia. Salah satu contoh algoritma kunci publik adalah algoritma McEilece. Algoritma McEilece adalah algoritma yang menggunakan sifat acak (randomization) pada proses pengenkripsiannya dan menjadi kandidat post quantum cryptography. Dalam pengaplikasiannya algoritma ini menggunakan matriks sebagai elemen pembangkit kuncinya. Algoritma ini juga merupakan algoritma yang tingkat keamanannya tinggi karena proses pembangkitan kuncinya yang dapat dibilang rumit karena penggunaan matriks tadi. Oleh karena itu pada makalah ini akan dilakukan studi algoritma kunci publik McEliece ini.**

***Index Terms*—Algoritma Kunci Publik, McEliece, Kunci Publik, Kunci Privat, Matriks**

I. PENDAHULUAN

Kriptografi merupakan ilmu atau seni untuk menjaga kerahasiaan pesan yang dalam hal ini adalah informasi dengan cara mengubahnya ke bentuk yang sulit dimengerti maknanya. Hal ini bertujuan agar sebuah pesan yang disampaikan hanya akan dapat dimengerti oleh orang yang berhak untuk mengetahuinya saja, tidak ada pihak lain yang terlibat. Kriptografi ini telah digunakan sejak zaman dahulu pula, bangsa-bangsa pada peradaban kuno sudah memakainya seperti mesir pada ribuan tahun yang lalu dan juga peradaban lainnya yang telah menggunakan konsep kriptografi dalam menyamarkan pesan rahasia dalam strategi perang.

Ilmu kriptografi semakin banyak digunakan dan mulai berubah menjadi kebutuhan utama. Dengan maraknya perkembangan ilmu teknologi informasi keamanan pun menjadi penting dan keamanan tidak hanya sekedar pada media tulis saja. Banyak teknologi-teknologi baru yang menyimpan informasi penting yang kita miliki dan tidak boleh jatuh ke tangan yang tidak berhak seperti nomor PIN dan *password*. Pada bidang inilah ilmu kriptografi dibutuhkan, agar informasi tersebut tidak jatuh ke tangan yang salah.

Salah satu contoh dari ilmu kriptografi adalah algoritma kunci publik atau algoritma kunci asimetri. Algoritma kunci asimetri adalah algoritma pengenkripsian dengan menggunakan kunci publik sebagai media penengkripsi dan kunci privat sebagai media pendekripsianya. Kunci publik digunakan oleh sang pemberi pesan untuk proses enkripsi dan pesan terenkripsi tersebut dikirimkan kepada sang penerima pesan bersama kunci privatnya yang dibangkitkan bersama kunci publiknya. Sang penerima pesan langung mendekripsi pesan tersebut menggunakan kunci privat yang diterima bersama pesan tadi.

Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan ke orang lain atau dapat dilihat oleh siapa saja. Sedangkan kunci privat adalah kunci yang dirahasiakan hanya orang-orang tertentu saja yang boleh mengetahuinya yaitu sang pemberi pesan dan juga sang penerima pesan. Kriptografi kunci-simetri dan kriptografi kunci-publik adalah dapat dianalogikan dengan kotak surat yang dapat dikunci dengan gembok. Anggap saja Alice dan Bob memiliki kunci gembok yang sama. Jadi Bob mengirimi Alice gembok dalam keadaan tidak terkunci. Analoginya adalah gembok merupakan kunci publik Bob dan kunci gembok merupakan kunci privat Bob.

Algoritma kunci publik ini pertama kali dipublikasikan oleh Diffie dan Hellman (ilmuan dari Stanford University) pada tahun 1976. Bentuk publikasinya adalah beberapa lembar karya tulis atau paper yang berjudul “New Directions in Cryptography”. Walaupun pada saat itu belum ditemukan algoritma kriptografi kunci-nirsimetri

yang sesungguhnya. Namun penemuan ini merupakan terobosan besar, karena pada saat itu masih menggunakan algoritma kunci simetri.

Algoritma McEliece adalah salah satu contoh algoritma kunci publiik yang pernah ditemukan. Algoritma McEliece ini merupakan algoritma yang unik karena algoritma ini menggunakan sifat acak (randomization) pada proses pengenkripsiannya. Algoritma ini merupakan algoritma yang menjadi kandidat post-quantum cryptography.

Dengan adanya algoritma kunci publik ini diharapkan nilai keamanan yang dijunjung tinggi bidang keilmuan kriptografi ini dapat terjaga dengan baik. Algoritma kunci publik ini digunakan untuk menutupi kelemahan dari algoritma sebelumnya yaitu algoritma kunci simetrik. Hal ini menunjukkan ilmu kriptografi akan terus berkembang dari zaman ke zaman sehingga walaupun dengan cepatnya persebaran informasi yang terjadi di dunia ini, keamanan dari informasi tersebut dapat lebih terjaga.

II. DASAR TEORI

Dalam algoritma McEliece terdapat teori yang melandasi algoritma tersebut. Pada bagian ini akan dijelaskan beberapa teori yang melandasi algoritma kunci publik tersebut.

2.1 Matriks

Dalam algoritma McEliece ini yang berperan sebagai kunci ataupun elemen pembangkitnya adalah matriks. Oleh karena itu pada bagian ini akan dijelaskan mengenai matriks lebih dalam.

Matriks adalah kumpulan bilangan berbentuk persegi panjang yang disusun menurut baris dan kolom. Bilangan-bilangan yang terdapat di suatu matriks disebut dengan elemen atau anggota matriks. Dengan representasi matriks, perhitungan dapat dilakukan dengan lebih terstruktur. Pemanfaatannya misalnya dalam menjelaskan persamaan linier, transformasi koordinat, dan lainnya. Matriks seperti halnya variabel biasa dapat dimanipulasi, seperti dikalikan, dijumlah, dikurangkan dan didekomposisikan.

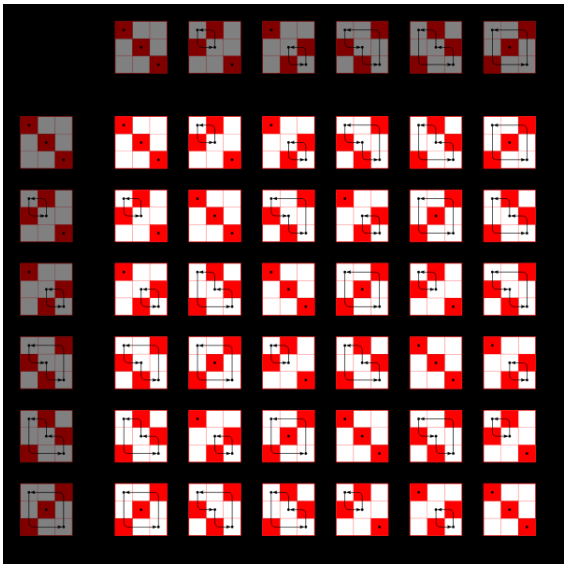
$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Gambar 2.1 Contoh Matriks

Namun pada algoritma McEliece ini elemen matriks yang digunakan bukanlah elemen matriks biasa, melainkan matriks yang elemennya diisi dengan bilangan biner yaitu 1 dan 0. Jenis matriksnya pun yang digunakan adalah yang khusus yaitu Permutation Matrix (Matriks Permutasi) dan Invertible Matrix (Matriks Invertible).

2.1.1 Matriks Permutasi

Matriks permutasi adalah matriks yang elemennya adalah bilangan biner. Syaratnya adalah hanya memiliki angka 1 di setiap baris dan di setiap kolomnya dan sisanya adalah angka 0. Untuk lebih jelasnya lihat gambar di bawah.



Gambar 2.2 Kombinasi dari matriks permutasi yang mungkin untuk ukuran 3x3

2.1.2 Matriks Invertible

Matriks Invertible adalah matriks yang memiliki invers. Syarat dari matriks ini adalah determinan dari matriks ini tidak sama dengan 0. Syarat yang lebih jelasnya adalah:

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n$$

Maksud dari rumus di atas adalah Jika matriks A dikalikan dengan matriks B hasilnya akan sama dengan matriks B dikalikan dengan matriks A yaitu matriks identitas. Hal ini menunjukkan bahwa matriks A dan matriks B saling inverse.

2.2 McEliece Cryptosystem

McEliece Cryptosystem atau algoritma McEliece adalah algoritma kunci asimetrik yang dikembangkan oleh Robert McEliece pada tahun 1978. Algoritma ini merupakan skema pertama yang menggunakan sifat acak (randomization) pada proses penengkripsiannya. Algoritma ini kurang mendapat perhatian di komunitas kriptografi walaupun algoritma ini merupakan candidat dari 'post-quantum cryptography'.

Dasar dari algoritma ini adalah dari sulitnya melakukan proses decoding kode linear. Sebagai gambaran pada kunci privat terdapat error-correcting code yang dipilih sebagai algoritma decoding yang efisien dan mampu memperbaiki t errors.

III. STUDI ALGORITMA MCELIECE

Pada bagian ke-3 kita akan mempelajari algoritma McEliece lebih mendalam bagaimana prosesnya dan bagaimana cara menggunakannya.

3.1 Skema McEliece

McEliece meliputi tiga algoritma yaitu yaitu algoritma 'probabilistic key generation algorithm' dalam menghasilkan kunci publik dan kunci privat, algoritma 'probabilistic encryption algorithm' dan algoritma 'deterministic decryption algorithm'. Pengguna dari algoritma ini menggunakan parameter tidak rahasia yaitu *n,k,*dan *t.*

Pembangkitan Kunci

1. Alice memilih kode linear biner *(n,k) C* yang mampu memperbaiki error *t.* Kode ini harus mampu berperan sebagai algoritma decoding yang efisien dan membangkitkan k x n matriks pembangkit *G* untuk kode *C.*
2. Alice memilih secara acak matriks invertibel biner dengan dimensi k x k, Matriks ini dinamakan dengan *S.*
3. Alice memilih secara acak matriks permutasi dengan dimensi n x n. Matriks ini dinamakan dengan *P.*
4. Alice menghitung matriks dengan dimensi k x n $\hat{G} = SGP.$
5. Kunci publik Alice adalah $(\hat{G}, t)$ dan kunci privatnya adalah (*S*,*G*,*P*).

Pengenkripsian Pesan

1. Bob melakukan encoding terhadap pesan *m* sebagai binary string dengan panjang *k.*
2. Bob menghitung vektor $c' = m\hat{G}.$
3. Bob membangkitkan *n*-bit vector *z* secara acak yang mengandung *t* (vektor dengan panjang *n* dan weight *t*)
4. Bob menghitung cipher teks $c = c' + z.$

Pendekripsian Pesan

1. Alice menghitung invers dari *P* (i.e. P^{-1}).
2. Alice menghitung $\hat{c} = cP^{-1}.$
3. Alice menggunakan algoritma decoding untuk code *C* untuk decoding $\hat{c}$ menjadi $\hat{m}.$
4. Alice menghitung $m = \hat{m}S^{-1}.$

3.2 Penggunaan McEliece

Pada bagian ini akan dijelaskan cara menggunakan algoritma McEliece ini sebagai algoritma enkripsi. Awalnya Alice akan mengirim pesan kepada Bob. Alice akan membangkitkan kunci terlebih dahulu. Misalnya setelah menggunakan algoritma decoding untuk menentukan n dan k (dalam hal ini menggunakan kode Hamming) didapat nilai n = 7 dan k = 4. Dari nilai tersebut ditentukan matriks G yaitu:

$$G = \begin{matrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{matrix}$$

Setelah itu bangkitkan matriks S secara acak dengan k = 4. Dengan kata lain dimensinya adalah 4 x 4. Didapat S:

$$S = \begin{matrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{matrix}$$

Setelah itu bangkitkan matriks P secara acak dengan n = 7. Dengan kata lain dimensinya adalah 7 x 7. Didapat P:

$$P = \begin{matrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}$$

Setelah itu hitung matriks $\hat{G} = SGP$:

$$G' = SGP = \begin{matrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{matrix}$$

Sebagai contoh, pesan yang hendak dikirimkan adalah m = (1 1 0 1) dalam bit. Panjang message menyesuaikan dengan nilai k. Misalnya panjangnya berlebih dipotong sejumlah k, dan misalkan panjangnya kurang dipadding hingga ukuran k.

Pesan dienkripsi dengan cara dikalikan dengan G'. Matriks hasil perkaliannya adalah (0 1 1 0 0 1 0) dan kemudian dijumlahkan dengan error vector dalam hal ini adalah z = (0 0 0 0 1 0 0). Maka Cipher teks yang terjadi adalah c = (0 1 1 0 1 1 0). dan

Setelah itu Bob menerima pesan c dan kunci privat yaitu (S,G,P). Bob langsung menghitung nilai c dikalikan dengan invers dari P. Dengan nilai inversnya adalah:

$$P^{-1} = \begin{matrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{matrix}$$

Hasil perkaliannya adalah c' = (1 0 0 0 1 1 1). Kemudian Bob melakukan decoding dengan menggunakan kode Hamming dan didapat m' = (1 0 0 0 1 1 0). Setelah itu diambil 4 digit pertamanya sesuai dan ghitung m dengan cara mengalikan dengan invers S yaitu:

$$S^{-1} = \begin{matrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{matrix}$$

Maka didapat nilai m = (1 1 0 1) sesuai dengan nilai m yang ditentukan Alice.

3.2 Serangan pada McEliece

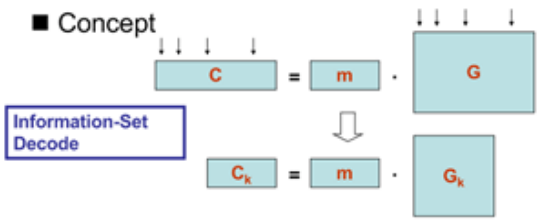
Hingga saat ini telah ditemukan serangan yang dilakukan untuk membongkar kerahasiaan pada algoritma McEliece ini.

Brute Force

Sang penyerang akan mencari tau nilai G dengan cara menggunakan Patterson algorithm. Ini tidak akan berhasil dengan mudah untuk nilai n dan t yan besar karena terlalu banyak kemungkinan untuk nilai G, S dan P.

Information Set Decoding

Algoritma Information Set Decoding (ISD) telah menjadi cara yang sangat efektif untuk menyerang algoritma McEliece dan algoritma Niederreiter yang merupakan pengembangan dari McEliece itu sendiri. Berbagai cara telah diperkenalkan. Cara yang paling efektif berdasarkan pencarian minimum atau kode yang pendek. Pada tahun 2008 Bernstein, Lange, dan Peters menggambarkan cara praktis untuk menyerang McEliece yang original dengan cara mencari kode low-weight menggunakan algoritma yang dipublikasikan oleh Jacquest Stern pada tahun 1989. Dengan menggunakan parameter yang disarankan oleh McEliece serangan dapat mencapae $2^{60.55}$ operasi bit.



Gambar 3.1 Skema ISD

IV. IMPLEMENTASI DAN ANALISIS

Pada bagian ini akan dijelaskan hasil dari implementasi algoritma McEliece ini.

4.1 Implementasi Aplikasi

Aplikasi Algoritma Kunci Publik McEilece ini diimplementasikan menggunakan library yang disediakan oleh www.flexiprovider.de dimana library ini berlisensi Open GPL. Namun yang diimplementasikan hanyalah pembangkit kuncinya saja khususnya dalah membangkitkan matriksnya, hal ini untuk menguji coba apakah membutuhkan waktu yang lama untuk membangkitkan suatu matriks. Ternyata dari hasil percobaan dalam membangkitkan kunci McEliece memakan waktu relatif lebih lama dibandingkan dengan membangkitkan kunci RSA. Di bawah akan disajikan file hasil keluaran dari aplikasi pembangkit matriks yang telah diimplementasikan. Nilai G yang didapat adalah:

```
1  4 7
2  1 0 0 0 1 1 0
3  0 1 0 0 1 0 1
4  0 0 1 0 0 1 1
5  0 0 0 1 1 1 1
6  Waktu:27.11
```

Gambar 4.1 Nilai Matriks G hasil pembangkitan kunci

Sedangkan untuk nilai S yang didapat adalah:

```
1  4 4
2  1 1 0 1
3  1 0 0 1
4  0 1 1 1
5  1 1 0 0
```

Gambar 4.2 Nilai Matriks S hasil pembangkitan kunci

Untuk nilai P yang didapat adalah:

```
1  7 7
2  0 1 0 0 0 0 0
3  0 0 0 1 0 0 0
4  0 0 0 0 0 0 1
5  1 0 0 0 0 0 0
6  0 0 1 0 0 0 0
7  0 0 0 0 0 1 0
8  0 0 0 0 1 0 0
```

Gambar 4.3 Nilai Matriks P hasil pembangkitan kunci

4.2 Analisis

Dari hasil implementasi dan studi yang dilakukan dapat dianalisis bahwa algoritma ini lebih rumit dibandingkan algoritma kunci publik lainnya seperti RSA dan Elgamal. Untuk membangkitkan suatu kunci saja membutuhkan waktu lebih dari 30 detik dalam pembangkitan kuncinya saja. Hal ini mungkin disebabkan dari algoritma decoding yang dipilih bukanlah algoritma decoding yang efisien. Dalam hal ini algoritma decoding yang digunakan adalah kode hamming.

V. KESIMPULAN

- Algoritma kunci publik atau algoritma asimetrik merupakan pengembangan dari algoritma sebelumnya yaitu algoritma simetrik yang dianggap tingkat keamanannya kurang karena kuncinya hanya boleh diketahui sang pengirim pesan dan juga sang penerima.
- Algoritma McEliece merupakan algoritma yang unik karena algoritma ini adalah algoritma pertama yang menggunakan sifat acak (randomization) pada proses pengenkripsiannya. Algoritma ini merupakan algoritma yang menjadi kandidat post-quantum cryptography.
- Pembangkitan kunci menggunakan algoritma McEliece lebih lama dibandingkan pembangkitan kunci menggunakan algoritma RSA dan Elgamal.

REFERENSI

[1] Munir, Rinaldi. 2006. "Diktat Kuliah IF5054 Kriptografi". Program Studi Teknik Informatika, Institut Teknologi Bandung.

[2] http://en.wikipedia.org/wiki/McEliece_cryptosystem

[3] http://en.wikipedia.org/wiki/Matrix_(mathematics)

[4] http://www.flexiprovider.de/

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Mei 2011

Widhaprasa Ekamatra Waliprana
13508080