Penggunaan Fingerprint Sebagai Kunci Privat Pada Algoritma El Gamal

Benedikus Holyson Tjuatja – 13510101
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510101@std.stei.itb.ac.id

***Abstract*—Pada makalah ini akan dibahas salah satu cara alternative dalam menentukan bilangan privat pada algoritma Elgamal. Cara yang diusulkan untuk mencapai tujuan ini adalah dengan melakukan bentuk sidik jari dari pengguna sebagai pembangkit kunci publik dan kunci privat. Sidik jari ini akan berfungsi untuk membentuk kunci privat pada fungsi Elgamal dan nantinya digunakan sebagai kunci dalam melakukan dekripsi. Pada pembuatan makalah ini juga dibuat sebuah program sederhana dengan menggunakan bahasa C#.**

Kata Kunci: kriptografi modern, sidik jari, Elgamal , Kunci privat.

I. PENDAHULUAN

Komunikasi merupakan salah satu cara yang digunakan oleh makhluk hidup untuk dapat berinterkasi dengan makhluk lainnya, hewan, manusia, tumbuhan pasti melakukan komunikasi. Setiap makhluk hidup ini memiliki cara tersendiri dalam berkomunikasi antara satu dengan yang lainnya. Cara berkomunikasi ini juga menggunakan berbagai cara, mulai dari cara yang sederhana atau langsung seperti dengan menggunakan suara ataupun gerak tubuh, hingga dengan cara yang kompleks atau tidak langsung seperti gerakan isyarat. Komunikasi ini merupakan kumpulan berbagai macam pola atau gerakan yang tersusun secara rapi dan beraturan, dan tentu saja pola ini harus dapat dimengerti oleh orang yang menjadi lawan bicaranya. Seiring berjalannya waktu cara berkomunikasi pun makin berkembang, dulu yang ketika berkomunikasi dua orang harus bertemu secara langsung, kini dapat dilakukan dengan jarak jauh. Cara berkomunikasi jarak jauh inipun kemudian berkembang terus, jarak komunikasi meningkat dan waktu yang dibutuhkan antar komunikasipun semakin singkat. Dimulai dari pengiriman pesan tertulis dengan surat dengan burung merpati sebagai kurir yang membutuhkan waktu bulanan untuk saling bertukar pesan, lalu berkembang menjadi pengiriman pesan suara dengan menggunakan telepon yang dapat dilakukan dalam hitungan detik, hingga akhirnya saat ini kita dapat saling bertukar citra dan suara menggunakan *video call* dengan jaringan internet sebagai penghubungnya. Semua perkembangan ini terjadi agar mempermudah hubungan komunikasi antara satu individu dengan individu lainnya.

Komunikasi jarak jauh ini kemudian menimbulkan suatu permasalahan baru yaitu bagaimana kita tahu bahwa kita telah melakukan komunikasi dengan lawan bicara yang kita harapkan, atau bagaimana kita tahu bahwa komunikasi ini tidak juga tidak dinikmati oleh orang yang tidak berkepentingan. Karena komunikasi terjadi apabila pihak penerima pesan mengerti makna dari pesan yang dikirimkan, maka orang-orang mulai melakukan pengkodean terhadap pesan yang dikirimkan hingga hanya orang tertentu yang mengetahui tentang kode itulah yang dapat mengerti isi pesan tersebut. Seni untuk mengubah pesan biasa menjadi kumpulan kode inilah yang kemudian disebut dengan kriptografi. Beda bentuk informasi yang ingin disampaikan beda pula cara pengembunyian pesan yang dilakukan.

Pada kriptografi klasik, pesan yang ingin dikodekan umunya berupa pesan fisik (tulisan di atas kertas), oleh karena itu pengkodean yang dilakukan adalah dengan menggunakan cara substitusi dan transposisi. Pada kriptografi modern pesan yang ingin dikodekan berupa pesan digital, oleh karena itu cara pengkodean biasanya adalah dengan mengubah isi bit-bit pembentuk pesan tersebut. Salah satu cara metode pengkodean yang dilakukan adalah dengan menggunakan sistem kunci privat dan kunci publik. Ide dari sistem ini secara umum adalah dengan melakukan enkripsi dengan menggunakan kunci publik lalu pendekripsian dilakukan dengan menggunakan kunci privat. Kunci privat dan kunci pulik ini memiliki dua nilai yang berbeda namun saling berhubungan, sehingga hanya orang yang mengetahui nilai kunci privatnya yang bisa membaca pesan yang dienkripsi dengan kunci publiknya. Salah satu cara untuk menghasilkan nilai kunci privat dan publik ini adalah dengan menggunakan algoritma elgamal. Semakin besar nilai dari kunci privat yang dibentuk maka semakin besar usaha yang dibutuhkan untuk melakukan pendekripsian pesan. Namun besarnya nilai kunci privat ini membuat orang sulit untuk menyimpan atau menghafal nilainya, oleh karena itu dibutuhkan suatu cara agar dapat membuat nilai privat tersebut susah untuk dipecahkan namun sederhana untuk diingat dan digunakan. Solusi yang

ditawarkan disini adalah dengan menggunakan sidik jari sebagai pembangkit kunci privat tersebut. Hal ini disebabkan karena setiap sidik jari manusia memiliki pola yang unik dan rumit sehingga cocok digunakan sebagai salah satu komponen dalam membuat *password* ataupun sistem pengamanan lain yang bersifat pribadi.

II. STUDI LITERATUR

Kriptografi dengan menggunakan kunci privat dan kunci publik ini juga disebut dengan kriptografi asimetrik. Metode ini membutuhkan dua buah nilai yang berbeda, masing-masing merepresentasikan kunci publik dan kunci privat, namun nilai dari dua buah kunci ini masih berhubungan. Kunci publik digunakan untuk melakukan enkripsi atau validasi suatu tanda tangan digital, sedangkan kunci privat digunakan sebagai kunci dekripsi atau pembuat tanda tangan digital. Kunci publik ini biasanya disebar dan digunakan oleh orang lain untuk melakukan enkripsi pesan yang akan ditujukan kepada pemilik kunci publik tersebut. Pesan itu kemudian didekripsi dengan menggunakan kunci privat yang dimilikinya, jika hasil dekripsi membentu suau pesan yang bermakna maka dapat dikatakan bahwa pesan tersebut memang ditujukan untuk dirinya. Pembentukan kunci publik ini sendiri didasarkan dengan kunci privat yang digunakan. Pembuatan nilainya biasa didasarkan pada persamaan-persamaan matematikan seperti faktorisasi, alogritma persamaan diskrit, dan kurva lingkaran. Kekuatan dari metoda ini terletak pada sulitnya (hampir tidak mungkin) untuk membentuk atau mincari nilai dari kunci privat berdasarkan pada kunci publiknya. Oleh karena itu biasanya kunci publik dapat disebarkan secara bebas sedangkan kunci privat tidak diedarkan karena digunakan untuk membaca pesan yang dienkripsi dengan kunci publik.

Elgamal adalah salah satu algoritma kriptografi yang memanfaatkan sistem algoritma kunci enkripsi asimetris. Keamanan dari algoritma ini terletak pada sulitnya menghitung nilai dari logaritma diskrit. Alogritma Elgamal ini dikemukakan oleh Taher Elgamal, seorang kriptografer Mesir, pada tahun 1985 di dalam makalah berjudul "*A public key cryptosystem and a signature scheme based on discrete logarithms*". Pada algoritma elgamal ini terdapat beberapa nilai yang harus dibuat, yaitu :

1. Nilai p
2. Bilangan g
3. Bilangan x
4. Nilai y
5. Pesan m
6. Chiper teks a dan b

P adalah bilangan bulat prima yang tidak rahasia atau dapat diberitahukan kepada publik. Bilangan g adalah suatu bilangan acak positif dengan nilai g lebih kecil daripada nilai p, nilai g dapat diberitahukan kepada publik. Bilangan x adalah bilangan acak positif yang memiliki nilai lebih kecil dibandingkan nilai p, bilangan ini bersifat rahasia dan merupakan kunci privat. Nilai y merupakan nilai dari kunci publik yang didapat dengan menggunakan persamaan :

$$y = g^x \bmod p$$

Kemudian nilai m yang merupakan nilai dari pesan yang ingin dienkripsikan, tentu saja nilai m ini bersifat rahasia. Kemudian nilai a dan nilai b merupakan hasil *chipper* dari pesan yang telah dienkripsi dengan kunci privat. Nilai a dan b merupakan pasangan hasil chipper pesan, oleh karena itu besar dari chipper teksnya akan selalu 2 kali lebih besar dibandingkan dengan besar *plain* teksnya.

Executable file (.exe) merupakan suatu ekstansi umum yang digunakan sebagai penanda utma dalam melakukan eksekusi suatu program. File executable terdiri dari kumpulan suatu binary yang mnyusun perintah-perintah untuk menjalankan suatu program. Selain hal tersebut data binary ini sendiri mengandung informasi lain seperti nilai jenis aplikasi, grafik bitmap dan ikon yang digunakan sebagai untuk membentuk tampilan antarmuka kepada pengguna.

Algoritma atau langkah dalam membangkitkan nilai kunci pada algoritma elgamal adalah sebagai berikut :

1. Penentuan nilai prima sembarang *p*
2. Menentukan nilai bilangan acak g dengan syarat nilai g lebih kecil dari nilai p
3. Menentukan nilai bilangan acak x dengan syarat nilai x terletak pada, $1 \leq x \leq p\text{-}2$
4. Melakukan perhitungan nilai *y* dengan menggunakan persamaan $y = g^x \bmod p$

Dari hasil algoritma ini akan terbentuklah nilai kunci publik yaitu nilai y, nilai g, dan nilai p, dan nilai dari kunci privat yaitu nilai x dan nilai p.

Algoritma atau langkah dalam melakukan enkripsinya sendiri adalah sebagai berikut :

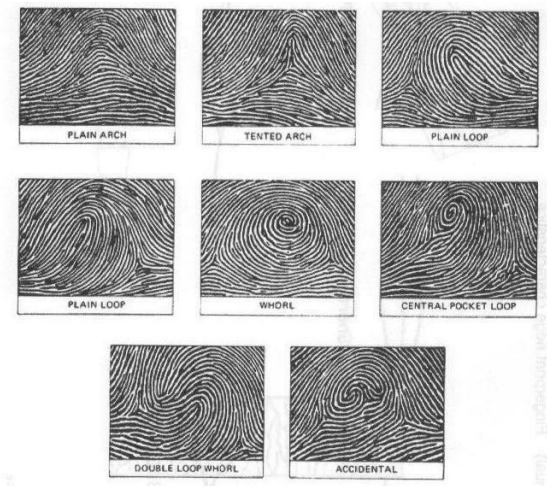
1. Menyusun nilai plainteks pesan m menjadi blok-blok $m_1, m_2, \ldots, m_n$, dimana nilai setiap blok m_n berada diantara selang nilai 0 hingga p-1
2. Pilih nilai bilangan acak k dalam hal ini nilainya berada pada $1 \leq k \leq p\text{-}2$
3. Setiap blok tersebut kemudian dienkripsi dengan persamaan $a = g^k \bmod p$ dan $b = y^k m \bmod p$.

Algoritma pada saat melakukan dekripsinya adalah sebagai berikut :

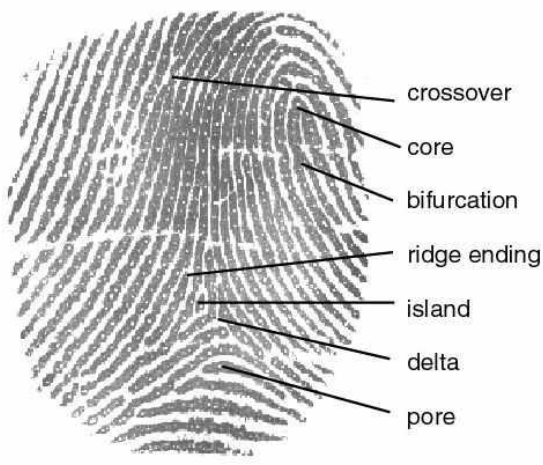
1. Dengan menggunakan kunci privat *x* , kemudian dihitung nilai dari $(a^x)^{-1} = a^{p-1-x} \bmod p$
2. Kemudian dilakukan penghitungan blok pesan plainteks *m* dengan menggunakan persamaan $m = b/a^x \bmod p = b(a^x)^{-1} \bmod p$

Fingerprint atau sidik jari adalah suatu jejak pola yang dihasilkan berdasarkan bentuk permukaan dari jari manusia. Setiap sidik jari yang ditinggalkan oleh masing-masing individu manusia memiliki pola yang berbeda dengan lainnya. Masing-masing jari memiliki bentuk sidik yang berbeda-beda pula. Keunikan dari sidik jari ini dapat

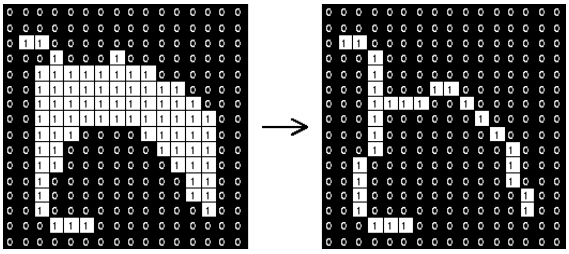
dijadikan sebagai salah satu ciri khas dari manusia tersebut. Oleh karena itu sidik jari manusia ini dapat bertindak sebagai password pada beberapa hal. Sidik jari ini memiliki pola-pola tersendiri secara keseluruhan, beberapa diantaranya adalah *Plain Arch, Tented Arch, Plain Loop, Whorl, Central Pocket Loop, Double Loop Whorl, Accidental.*



Dari pola ini kemudian dicari beberapa paremeter yang dapat membedakan dua buah sidik jari yang berbeda namun memiliki pola keseluruhan yang sama. Terdapat beberapa bentuk parameter pembeda yang dicari seperti posisi ujung garis, cabang, titik, titik belok, dan lain-lain. Antar sidik jari ini akan memiliki posisi dan jumlah dari tiap parameter yang berbeda-beda.



Dari gambar sidik jari yang didapat kemudian dibutuhkan suatu algoritma yang dapat mengolah gambar tersebut untuk mendapatkan pola-pola parameter ini. Salah satu cara pengolahan citra untuk mendapatkan parameter ini adalah dengan menggunakan suatu algoritma penipisan. Tujuan dari algoritma penipisan ini adalah untuk melakukan eliminasi dan mengurangi ketebalan dari suatu garis sehingga gambar yang diolah akan menghasilkan satu garis tipis. Garis tipis ini kemudian akan diolah kembail untuk mendapatkan parameter yang dibutuhkan dalam proses pengenalan suatu citra. Dalam hal ini, citra yang telah ditipiskan akan diproses kembali untuk mendapatkan parameter pembeda yang membuat unik suatu bentuk sidik jari.



III. RANCANGAN

Ide utama dalam pada makalah ini adalah bagaimana cara agar kunci privat dan kunci publik yang akan digunakan seseorang dalam melakukan pertukaran pesan dapat menjamin kerahasiaan suatu pesan dan mudah untuk diproses atu digunakan oleh pengguna. Seperti yang telah dibahas sebelumnya, cara pembentukan kunci privat dan kunci publik inilah memegang peranan penting dalam menjaga keamanan dari pesan yang akan dikirimkan. Pada umumnya, cara biasa dalam penentuan nilai dari kunci privat dan kunci publik ini dilakukan secara acak. Sistem ini biasanya digunakan hanya untuk menjaga keamanan komunikasi dalam satu sesi saja. Kunci privat dan kunci publik ini akan dibuat ulang kembali ketika akan melakukan sesi percakapan berikutnya. Namun pertukaran data ini cenderung kurang praktis karena kedua belah pihak yang saling berhubungan harus menunggu pihak lainnya untuk mengirimkan kunci publik yang akan digunakan pada sesi tersebut. Ketika suatu komunikasi terputus atau salah satu lawan komunikasi ingin menggunakan device yang berbeda, maka sesi tersebut harus diputus dan kemudian akan dibentuk suatu sesi komunikasi yang baru. Dari hal ini muncul suatu ide bagaimana cara tetap menyimpan nilai dari kunci privat dan publik seseorang tanpa terikat pada device tertentu. Dengan memanfaatkan sidik jari manusia sebagai faktor pembentuk kunci privat dan kunci publik, maka proses pembentukannya tidak lagi dilakukan secara acak namun berdasarkan sidik jari tersebut.

Seperti yang telah dibahas sebelumnya, banyak faktor pada sidik jari yang dapat dijadikan pedoman dalam melakukan pembangkitan nilai kunci privat dan kunci publik. Posisi dan jumlah dari titik belok, pulau, titik ujung, titik cabang dan sebagainya yang terdapat pada sidik jari ini dapat dimanfaatkan sebagai faktor dalam membangkitkan nilai dari kunci privat dan kunci publik. Pada makalah ini hanya jumlah dan posisi dari titik cabang dan titik ujung yang akan digunakan dalam pembentukan nilai dari kunci privat dan kunci publik. Untuk mendapatkan posisi dan jumlah ini akan dilakukan dua tahap pengolahan citra terlebih dahulu. Tahap pertama adalah dilakukan penipisan citra sidik jari tersebut agar pengambilan data menjadi lebih sederhana

dan lebih mudah. Penipisan citra ini dilakukan dengan menggunakan *thinning algorithm* sederhana. Tahap kedua adalah penentuan titik citra apakah titik tersebut merupakan titik cabang atau titik ujung.

Pengujian pada makalah ini dilakukan dengan membuat suatu program sederhana yang dapat memproses suatu citra dari sidik jari sederhana yang kemudian akan dibangkitkan nilai dari kunci privat dan kunci publik berdasarkan data yang diperoleh dari pengolahan citra tersebut. Program ini dibuat dengan menggunakan kakas Microsoft Visual Studio 2010 yang menggunakan bahasa pemrograman C#. Selain menggunakan algoritma kriptografi, pada program ini juga akan menggunakan beberapa algortma pengolah citra yang akan digunakan dalam mengolah citra dari sidik jari yang digunakan.

IV. IMPLEMENTASI

Seperti yang telah dibahas pada tahap rancangan, implementasi dari makalah ini akan menggunakan bahasa pemrograman C# dengan melakukan tiga buah tahap. Proses pengolahan ini juga terdiri dari dua tahap, yiatu tahap enkripsi pesan dan tahap dekripsi pesan yang telah dienkripsi. Secara umum program yang dibuat akan mengolah sebuah citra sidik jari, kemudian membangkitkan nilai kunci privat dan kunci publik berdasarkan citra tersebut, lalu melakukan enkripsi dan dekripsi kunci tersebut dengan menggunakan algoritma elgamal.

A. Pengolahan Citra

Pengolahan citra ini dilakukan dengan tujuan untuk mendapatkan jumlah dan posisi parameter-parameter yang akan digunakan pada tahap pembangkitan kunci dari gambar sidik jari yang diberikan. Pada makalah ini parameter yang dicari sederhana yaitu titik ujung dan titik cabang dari garis sidik jari. Untuk kedepannya parameter untuk membangkitkan kunci ini dapat ditambah seperti pulau, titik belok, dan lain-lain. Seperti yang telah dibahas sebelumnya proses pengolahan citra ini dilakukan secara dua tahap, yaitu proses penipisan garis sidik jari dan proses penentuan parameter. Asumsi yang diberikan pada pengolahan citra ini adalah, citra yang diberikan berupacitra yang telah diolah sehingga hanya terdapat dua warna yaitu hitam (RGB 0 0 0) dan putih (RGB 255 255 255). Citra yang diolah juga bersih atau tidak terdapat noise yang dapat mengganggu identifikasi gambar. Proses pertama yang dilakukan adalah penipisan citra sederhana berdasarkan kulit. Penipisan dilakukan dengan melakukan eliminasi kulit dari garis pada citra tersebut satu persatu hingga nantinya garis sidik jari tersebut hanya terbentuk dari 1 garis tipis saja. Proses ini dilakukan dengan penelusuran citra yang dilakukan secara perpixel. Penelusuran ini dilakukan hingga ditemukan suatu pixel yang berwarna hitam atau menandakan bahwa pixel tersebut merupakan bagian dari garis sidik jari. Ketika ketemu, maka akan dilakukan penulusuran daerah luar dari garis sidik jari tersebut. Penelusuran ini dilakukan dengan mengitari pixel terluar dari garis sidik jari tersebut, dan akan berhenti apabila pengitaran telah sampai pada titik awal. Setelah mendapatkan titik pengitarannya, maka pixel yang telah dilalui akan dihapus apabila terdapat lebih dari dua pixel berwarna hitam yang berada disekitarnya

```
for (int i = 0; i < gambar.Height; i++)
{
    for (int j = 0; j < gambar.Width; j++)
    {
        if (warna1[(i * gambar.Width) + j].R == 0)
        {
            // Proses pixel tersebut
            TanganKiriBasah32(j, i);
            // Hapus daerah yang dilalui
            checkStack.Add(i * gambar.Width + j);
            bomTugas32();

        }
    }
}
```

Titik-titik pixel yang ditelusuri dimasukan kedalam suatu list, yang kemudian akan dilihat apakah disekitar titik tersebut terdapat pixel berwarna hitam lainnya. Jika terdapat lebih dari 2 pixel tetangga yang berwarna hitam, maka dapat dikatakan bahwa titik tersebut belum membentuk suatu garis, sehingga titik tersebut akan dihapus.

```
while (checkStack.Count > 0)
{
    // Ambil pixel yang ditelusuri pertama
    int check = checkStack[0];
    checkStack.RemoveAt(0);
    int i = check / gambar.Width;
    int j = check % gambar.Width;
    int count = 0;
    for (int k = i - 1; k < i + 2; k++)
    {
        if (k >= 0 && k < gambar.Height)
        {
            for (int l = j - 1; l < j + 2; l++)
            {
                if (l >= 0 && l < gambar.Width)
                {
                    if (warna1[(k * gambar.Width) + l] == Color.Black)
                    {
                        count++;
                    }
                }
            }
        }
    }
    if (count > 3)
    {
        warna1[check] = Color.White;
    }
}
```

Proses penulusuran ini akan dilakukan lagi untuk menghapus kulit selanjutnya, hingga akhirnya objek yang dilewati berupa sebuah garis dengan ketebalan 1 pixel. Proses penipisan ini akan berhenti apabila semua garis yang terdapat pada citra tersebut telah memiliki ketebalan 1pixel.

Ketika telah terbentuk suatu citra baru dengan penipisan yang telah dilakukan sebelumnya, maka tahap

berikutnya adalah pencarian titik-titik yang menjadi parameter yang akan digunakan dalam pembangkitan kunci privat dan kunci publik. Cara penentuan ini adalah dengan menelusuri kembali citra tersebut secara perpixel. Proses akan dilakukan apabila ditemukan suatu pixel yang berwarna hitam.

```
for (int i = 0; i < gambar.Height; i++)
{
    for (int j = 0; j < gambar.Width; j++)
    {
        if (warna1[(i * gambar.Width) + j].R == 0)
        {
            // Proses pixel tersebut
            processPixel(j, i);
        }
    }
}
```

Pixel tersebut kemudian akan dilihat apakah disekitar pixel tersebut hanya terdapat 1 buah pixel tetangga yang berwarna hitam. Jika benar, maka hal ini dapat dikatakan bahwa pixel tersebut merupakan suatu titik ujung dari suatu garis. Perlu diketahui disini, dengan algoritma penipisan yang digunakan maka titik cabang yang menjadi parameter ini akan terhapus dan berubah menjadi 3 buah titik ujung yang baru.

```
int count = 0;
for (int k = i - 1; k < i + 2; k++)
{
    if (k >= 0 && k < gambar.Height)
    {
        for (int l = j - 1; l < j + 2; l++)
        {
            if (l >= 0 && l < gambar.Width)
            {
                if (warna1[(k * gambar.Width) + l] == Color.Black)
                {
                    count++;
                }
            }
        }
    }
}
if (count <= 2)
{
    // Merupakan titik ujung
    titikUjung.Add(new Point(j, i));
}
```

Proses ini berhenti apabila semua pixel pada citra tersebut telah diperiksa. Hasil dari pemrosesn ini adalah suatu list titik-titik yang akan digunakan untuk membangkitkan nilai kunci privat dan kunci publik.

B. Pembangkitan Kunci

Seperti yang telah dibahas sebelumnya proses enkripsi dan dekripsi ini akan menggunakan algoritma elGamal, sehingga proses pembangkitan kunci ini juga akan didasarkan pada algoritma tersebut. Pada algorimta elGamal terdapat beberapa nilai yang harus dicara dalam menentukan kunci publik dan kunci privat. Untuk kunci publik membutuhkan nilai tripel (y, g, dan p) dan untuk kunci privat membutuhkan nilai pasangan (x dan p). Proses penentuan kunci privat dan kunci publik pada makalah ini akan sedikit dibalik. Pada makalah ini, list posisi sidik jari yang didapat sebelumnya digunakan untuk membentuk nilai x yang akan digunakan sebagai kunci privat. Pembuatan nilai x pada makalah ini tergolong sederhana, yaitu dengan menggabungkan semua posisi sidik jari yang didapat sebelumnya menjadi satu buah tipe bilangan big integer yang panjang.

```
for (int i = 0; i < titikUjung.Count; i++)
{
    temp += titikUjung[i].X.ToString()
        + titikUjung[i].Y.ToString();
}
BigInteger x = new BigInteger(temp);
```

Setelah mendapatkan nilai x, baru dicari nilai bilangan prima p yang memiliki nilai lebih besar dibandingkan dengan nilai x ini.

```
BigInteger p;
bool done = false;
while (!done)
{
    p = new BigInteger(createRandomBigInt().ToString());
    if (isPrime(p) && isBiggerThanX(p))
    {
        done = true;
    }
}
```

Setelah mendapa nilai p, lalu akan dicari nilai g yang merupakan bilangan random dengan syarat nilai berada di bawah nilai bilangan prima p.

```
BigInteger g;
done = false;
while (!done)
{
    g = new BigInteger(createRandomBigInt().ToString());
    if (isLessThanP(g))
    {
        done = true;
    }
}
```

Setelah mendapatkan nilai big integer g, x, dan p akan dilakukan pencarian nilai y dengan menggunakan persamaan $y = g^x \bmod p$.

```
BigInteger y;
y = pangkat(g,x).Mod(p);
```

C. Enkripsi dan Dekripsi

Setelah menemukan nilai kunci privat dan kunci publik, maka akan diterapkan enkripsi dan dekripsi standar yang menggunakan algorimta elGamal. Pada proses enkripsi dilakukan pencarian nilai a dan b, yang kemudian akan menjadi hasil pesan chipper untuk blok pesan m. Pesan

sebelumnya akan dibagi menjadi blok-blok yang memiliki ukuran lebih kecil disbanding dengan nilai p. Semakin besar nilai p, maka semakin besar pesan yang disimpan dalam satu blok. Sebelum dienkripsi akan dicari dulu suatu nilai bilangan acak k yang nantinya akan menentukan hasil pesan enkripsi dan nilai k sendiri harus lebih kecil dibandingkan dengan nilai p.

```
for (int i = 0; i < blokPesan.Count; i++)
{
    BigInteger k;
    done = false;
    while (!done)
    {
        k = new BigInteger(createRandomBigInt().ToString());
        if (isLessThanP(k))
        {
            done = true;
        }
    }

    BigInteger a;
    a = pangkat(g, k).Mod(p);
    BigInteger b;
    b = pangkat(y, k).Multiply(blokPesan[i]).Mod(p);
    chipperA.Add(a);
    chipperB.Add(b);
}
```

Seperti yang diketahui sebelumnya, karena hasil enkripsi adalah berupa pasangan nilai a dan b, maka ukuran pesan chipper akan menjadi dua kali lebih besar dibandingkan pesan sebenarnya.

Pada proses dekripsi akan diolah kembali pesan chipper A dan pesan chipper B menjadi pesan biasa dengan menggunakan kunci privat x. Blok-blok pesan hasil dekripsi kemudian akan digabung kembali menjadi pesan aslinya.

```
for (int i = 0; i < chipperA.Count; i++)
{
    BigInteger ax;
    ax = getAx(chipperA[i], p);

    pesan += chipperB[i].Multiply(ax).Mod(p);
}
```

V. Analisis Hasil

Dari percobaan yang dilakukan didapatkan hasil yang sesuai dengan yang diharapkan. Kunci publik berhasil dihasilkan dengan baik dan dapat merubah pesan bermakna menjadi blok-blok pesan yang terenkripsi. Proses dekripsi pengembalian hasil pesan terenkripsi dengan menggunakan kunci privat juga berhasil dilakukan. Pembuatan kunci privat dan kunci publik dengan menggunakan citra sidik jari dapat menghasilkan suatu deretan angka yang memiliki tingkat kerumitan yang cukup bagus. Meskipun pada percobaan kali ini tidak menggunakan semua pola sidik jari, hasil yang diberikan telah cukup mencapai target. Pengolahan citra sidik jari yang dilakukan juga tergolong sederhana dengan dilakukan pembersihan citra sidik jari secara manual sebelumnya. Kedepannya diharapkan pembentukan nilai kunci privat dan kunci publik ini dapat menggunakan seluruh parameter yang mungkin pada sidik jari. Perangkat keras juga diharapkan untuk dikembangkan agar pengambilan citra sidik jari dapat dilakukan secara langsung dan cepat.

VI. Kesimpulan

Pembangkitan nilai kunci publik dan kunci privat berdasarkan sidik jari mungkin untuk dilakukan. Pengiriman dan pembacaan pesan dengan menggunakan sidik jari akan memberikan jaminan lebih bahwa pesan tersebut hanya dapat dibaca oleh orang yang dituju. Namun dibutuhkannya perangkat keras yang mendukung pembacaan pola sidik jari agar mencegah pembacaan pesan dengan menggunakan citra sidik jari orang lain.

References

[1] J. Katz; Y. Lindell (2007). *Introduction to Modern Cryptography*. CRC Press. ISBN 1-58488-551-3.

[2] Taher ElGamal (1985). "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". *IEEE Transactions on Information Theory* **31** (4): 469–472.

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, 18 Mei 2014

ttd

Benedikus Holyson Tjuatja
13510101