Aplikasi Persamaan Diophantine dalam Kriptografi

Lydia Astrella Wiguna 13517019
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517019@std.stei.itb.ac.id

***Abstrak* — Persamaan Diophantine dalam teori bilangan adalah persamaan untuk mendapatkan solusi bilangan bulat untuk koefisien-koefisien dalam polinom. Persamaan ini dapat digunakan untuk membentuk algoritma kriptografi yang dibutuhkan untuk menjaga keamananan data. Perkembangan keamanan data melalui kriptografi semakin dibutuhkan seiring dengan teknologi informasi yang turut berkembang. Algoritma kriptografi mengubah data menjadi sandi serta mengubah kembali sandi tersebut menjadi data dengan menggunakan kunci. Pada makalah ini akan dibahas aplikasi persamaan Diophantine dalam pembentukan kunci.**

***Kata Kunci* — Algoritma Kriptografi, Kriptografi, Persamaan Diophantine**

I. PENDAHULUAN

Seiring dengan kemajuan teknologi informasi yang pesat, semakin maju, banyak, dan beragam pula kejahatan sistem komputer seperti pencurian data, mata-mata atau spionase, pemalsuan data, dan sebagainya. Maka dari itu dibutuhkan pengamanan sistem komputer yang meliputi pengamanan data dan pengamanan jaringan. Data yang aman hanya bisa diakses dan dibaca oleh pihak yang memang berwenang atas data tersebut, hanya bisa diubah oleh pihak yang berhak, dan hanya tersedia dan dapat dimanfaatkan oleh pihak-pihak berwenang tersebut.

Sistem kriptografi memungkinkan jaminan keamanan sistem komputer. Kriptografi memiliki dua buah komponen yang utama yaitu algoritma kriptografi dan kunci. Algoritma kriptografi merupakan metode-metode yang digunakan untuk menjaga keamanan dengan cara mengubah bentuk data ke dalam bentuk sandi terlebih dahulu sebelum dikirim melalui jaringan yang tidak terpercaya. Ketika data yang sudah disandikan tersebut diterima barulah diterjemahkan kembali ke bentuk data semula. Dalam proses pengubahan data menjadi sandi dan pengubahan sandi menjadi data dibutuhkan kunci yang digunakan dalam algoritma kriptografi. Kunci yang dirahasiakan ini yang menjamin keamanan data.

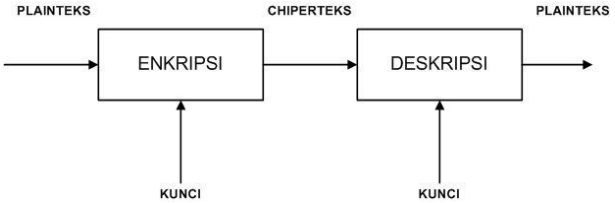
Algoritma kriptografi dan kunci yang digunakan pada saat ini sangat beragam. Contoh algoritma kriptografi yang sering dipakai saat ini adalah Rivest-Shammir-Adleman (RSA), Elliptic Curve Cryptography (ECC), dan lain-lain. Pada makalah ini akan dibahas penggunaan persamaan Diophantine untuk membentuk algortima kriptografi nirsimetri dan kunci.

II. KRIPTOGRAFI

A. Pengertian Kriptografi

Kriptografi adalah ilmu yang membahas metode-metode pengamanan pesan. Kriptografi banyak memanfaatkan konsep-konsep dari teori bilangan. Kriptografi sangat dibutuhkan untuk menjaga kerahasiaan data yang bersifat privat. Pengamanan pesan diaplikasikan pada kegiatan pengiriman pesan dan penyimpanan data. Pada pengiriman pesan, pesan yang akan dikirim diubah ke dalam bentuk sandi. Setelah diterima oleh pihak yang seharusnya menerima, sandi baru diubah kembali menjadi pesan semula. Sedangkan pada penyimpanan data, data yang disimpan sudah dalam bentuk sandi. Saat akan dibaca, sandi baru diubah kembali menjadi data semula.

Cara kerja metode pengamanan pesan pada kriptografi secara umum adalah menyandikan pesan biasa yang disebut plain (*plaintext)* menjadi kode-kode yang sulit dibaca dan tidak dapat diartikan yang disebut cipherteks (*ciphertext*). Penyandian plainteks menjadi cypherteks dinamakan enkripsi. Ketika pesan dibutuhkan oleh orang yang memang berhak, pesan yang masih berbentuk cipherteks tadi diubah menjadi bentuk plainteks kembali. Pengembalian bentuk cipherteks menjadi bentuk plainteks dinamakan dekripsi. Metode enkripsi dan dekripsi yang digunakan bergantung pada algoritma kriptografi yang dipakai. Pada masing-masing kegiatan enkripsi dan dekripsi membutuhkan kunci yang dirahasiakan atau sebagian dirahasiakan.



Gambar Alur Enkripsi dan Dekripsi
(sumber:https://mugi2sae.files.wordpress.com/2010/09/skema-enkripsi-deskripsi-visio.jpg diakses pada 8 Desember 2018 pukul 15.30)

Notasi matematika untuk enkripsi sebagai berikut,

$$E(P) = C$$

Dengan P adalah plainteks dan C adalah cipherteks. Sedangkan E adalah fungsi enkripsi yang berdomain plainteks dan

berdaerah hasil C. Notasi matematika untuk dekripsi sebagai berikut,

$$D(C) = P$$

Dengan D adalah fungsi dekripsi yang berdomain cipherteks dan berdaerah hasil plainteks. Fungsi dekripsi dan enkripsi harus berkoresponden satu-satu sehingga memenuhi

$$D(E(P)) = P$$

agar plainteks yang diubah menjadi cipherteks bisa kembali menjadi plainteks yang sama dengan plainteks awal.

Jenis sistem kriptografi berdasarkan jumlah kuncinya dibedakan menjadi dua yakni,

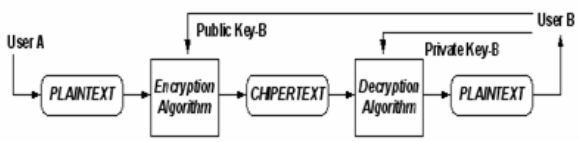
1. sistem kriptografi kunci simetri yang menggunakan algortima simetri
2. sistem kriptografi nirsimetri yang menggunakan algoritma nirsimetri.

Pada makalah ini hanya akan dibahas sistem kriptografi nirsimetri.

B. Sistem Kriptografi Nirsimetri

Sistem kriptografi nirsimetri disebut juga sistem kriptografi kunci publik. Sistem kriptografi ini menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Sistem ini disebut sistem kriptografi kunci publik karena salah satu kuncinya boleh disebarluaskan dan kunci yang lainnya harus dirahasiakan. Algoritma nirsimetri lebih sering dipakai modern ini karena lebih kuat daripada sistem kriptografi konvensional, sistem kriptografi kunci simetri yang hanya menggunakan satu buah kunci.

Kunci publik yang dapat disebarluaskan merupakan kunci enkripsi. Setiap orang bebas mengenkripsi dengan kunci enkripsi yang disebarkan. Kunci yang dijaga kerahasiaannya merupakan kunci untuk dekripsi yang disebut kunci privat.



Gambar Alur Enkripsi dan Dekripsi dengan Kunci Publik (sumber:https://rezqiwati.wordpress.com/2009/04/03/kriptografi-jaringan/ diakses pada 8 Desember 2018 pukul 19.00)

Notasi matematika untuk enkripsi dan dekripsi menjadi,

$$E_{Ke}(P) = C$$
$$D_{Kd}(C) = P$$

dengan Ke merupakan kunci publik dan Kd merupakan kunci privat.

Kriptanalis, orang yang berusaha memecahkan cipherteks menjadi plainteks dengan illegal akan kesulitan dengan sistem kriptografi nirsimetris karena tidak mengetahui kunci dekripsi yang berbeda dari kunci enkripsi.

C. Kekuatan Algoritma Kriptografi

Algoritma kriptografi mempunyai tiga aspek yang mengukur kekuatan algoritma kriptografi, sebagai berikut:

1. Kompleksitas Data

   Kompleksitas data mengukur banyak data yang diperlukan seorang kriptanalis untuk memecahkan algoritma. Semakin banyak data yang diperlukan, semakin terjamin kemanannya. Misalkan data cipherteks yang diperlukan untuk menerobos algoritma kriptografi dengan suatu kunci berjumlah 100. Sedangkan setiap kunci hanya dipakai sekali untuk satu pesan. Maka dapat dipastikan algoritma yang dipakai kuat.

2. Kompleksitas Proses

   Kompleksitas proses disebut juga faktor kerja. Kompleksitas proses mengukur lama waktu yang diperlukan untuk melakukan penerobosan algoritma oleh seorang kriptanalis. Semakin cepat waktu yang diperlukan semakin buruk. Misalkan jika dibutuhkan waktu lima tahun untuk menerobos suatu algoritma kriptografi. Sedangkan waktu pemakaian algoritma tersebut sebatas satu tahun. Maka algoritma yang dipakai suda cukup kuat.

3. Kebutuhan Memori

   Kebutuhan memori mengukur banyak memori yang dibutuhkan untuk menerobos algoritma. Semakin banyak memori yang dibutuhkan untuk menerobos algoritma kriptografi, akan semakin baik.

III. TEORI BILANGAN BULAT

Bilangan bulat adalah bilangan rasional yang termasuk dalam bilangan real yang tidak mempunyai pecahan decimal. Bilangan bulat memiliki simbol $\mathbb{Z}$. Contoh bilangan bulat (1, 2, 3, 58, 109, 0 , -4, -452, dan lain-lain). Contoh bilangan yang bukan termasuk ke dalam bilangan bulat (0.3, -43.2, dan lain-lain). Teori bilangan berfokus pada pembagian bilangan bulat.

A. Pembagian Bilangan Bulat

Misalkan a dan b adalah dua bilangan bulat dengan a tidak sama dengan 0. a habis membagi b jika terdapat bilangan bulat c sedemikian sehingga b = ac.

Notasi untuk a habis membagi b adalah:

$$a \mid b, a \neq 0$$

Hasil baginya berbentuk bilangan bulat. Artinya b merupakan kelipatan dari a karenanya selain a habis membagi b, sering pula disebut b kelipatan a.

Dalam bentuk umum, hasil dari pembagian bilangan bulat dengan biangan bulat positif lainnya dapat dinyatakan dengan hasil bilangan bulat dan sisa pembagian yang berupa bilangan bulat juga. Pada kasus a habis membagi b di atas termasuk kasus khusus di mana sisa pembagainnya bernilai 0.

Pembagian bilangan bulat secara umum dinyatakan :

$$m = nq + r$$

dengan m adalah bilangan bulat yang dibagi (*dividend)* , n adalah bilangan bulat pembagi (divisor), q adalah hasil pembagian dalam bentuk bilangan bulat (*quotient*), dan r adalah sisa pembagian dalam bentuk bilangan bulat positif (*remainder*).

Bentuk penggunaan operator div dan mod dalam pembagian bilangan bulat:

$$q = m \text{ div } n$$
$$r = m \text{ mod } n$$

Hasil dari operasi div adalah hasil pembagian, sedangkan hasil dari operasi mod adalah sisa pembagian.

B. Pembagi Bersama Terbesar

Pembagi bersama terbesar atau disebut juga *greatest common divisor* adalah faktor pembagi yang sama antara dua buah bilangan bulat yang merupakan bilangan pembagi terbesar dan berbentuk bilangan bulat juga. Contoh PBB (6,15) adalah 3 karena 3 habis membagi 6 dan habis membagi 15 dan juga merupakan faktor pembagi yang paling besar. 1 juga habis membagi 6 dan habis membagi 15 tetapi 3 lebih daripada 1. Karena itu nilai PBB yang dipilih adalah 3.

Berikut ini sifat-sifat yang berhubungan dengan PBB pada bilangan bulat a, b, dan c:

1. Misalkan c adalah PBB(a,b), maka c habis membagi a+b
2. Misalkan c adalah PBB (a,b), maka c habis mebagi a-b
3. Misalkan c habis membagi a, maka c habis membagi ab

Hubungan PBB dalam bentuk umum pembagian bilangan bulat :

$$m = nq + r, \ 0 \leq r < n$$

m dan n merupakan bilangan bulat dan memenuhi kondisi di atas. Maka berlaku hubungan:

$$PBB(m,n) = PBB(n,r)$$

C. Algoritma Euclidean

Selain cara manual dalam mencari nilai PBB, yaitu dengan mencari bilangan-bilangan yang habis membagi kedua nilai lalu mengambil nilai yang terbesar, terdapat cara lain untuk mendapatkan nilai PBB melalui algoritma Euclidean.

m dan n adalah bilangan bulat tak negatif dan $m \geq n$. $r_0 = m$ dan $r_1 = n$. Lalu dilakukan pembagian bilangan bulat secara terus menerus hingga dihasilkan sisa pembagian bernilai 0.

$$r_0 = r_1q_1 + r_2 \qquad 0 \leq r_2 < r_1$$
$$r_1 = r_2q_2 + r_3 \qquad 0 \leq r_3 < r_2$$
$$r_2 = r_3q_3 + r_4 \qquad 0 \leq r_4 < r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_nq_n + 0$$

Setelah merumuskan pembagian bilangan bulat secara terus-menerus sampai hingga sisa pembagian bernilai 0, dilihat hubungan PBB pada tiap-tiap pembagian bilangan bulat yang berlaku:

$$PBB(m,n) = PBB(r_0,r_1) = PBB(r_1,r_2) = PBB(r_3,r_4) = \ldots = PBB(r_{n-2},r_{n-1}) = PBB(r_{n-1},r_n) = PBB(r_n,0) = r_n$$

Dari hubungan PBB di atas, diperoleh nilai PBB adalah nilai pembagi bilangan bulat (*divisor*) terakhir saat sisa pmebagiannya (*remainder*) bernilai 0.

Secara terangkum, algoritma Euclidean memiliki langkah-langkah pengerjaan:

1. Ketika n = 0, PBB (m,n) bernilai m.
2. Ketika n bukan 0, PBB m dibagi dengan n, sisa pembagiannya misalkan r. Lalu ganti nilai m awal dengan nilai n dan nilai n awal dengan r. Analisis kembali dari langkah pertama.

Misalkan a dan b adalah bilangan bulat postif, maka PBB (a,b) dapat dinyatakan dalam bentuk:

$$PBB(a,b) = ma + nb$$

dengan m dan n bilangan bulat sebagai koefisien-koefisien kombinasi liniernya. Cara menemukan kombinasi linier seperti di atas dapat menggunakan algortima Euclidean untuk menemukan nilai PBB-nya. Lalu melakukan penelusuran langkah-langkah algoritma Euclidean yang sudah dibuat dengan cara melakukan subsbtitusi-substitusi nilai dan arahnya mundur hingga menemukan koefisien- koefisien dari a dan b.

D. Relatif Prima

Bilangan bulat a dan b dinyatakan relatif prima terhadap satu sama lain jika PBB (a,b) memiliki nilai 1. Oleh karena nilai PBB (a,b) = 1, maka bentuk persamaan liniernya menjadi:

$$ma + nb = 1$$

D. Aritmetika Modulo

Seperti sudah dijelaskan pada upabab A, operator untuk melakukan operasi modulo adalah mod yang menghasilkan sisa pembagian bilangan bulat. Misalkan a dan b adalah bilangan bulat positif hasil operasi a mod m adalah sisa hasil pembagian (*remainder*) a oleh m :

$$a \text{ mod } m = r$$
$$a = mq + r$$

dengan $0 \leq r < m$. m disebut modulo atau modulus. Jika a mod m bernilai 0, maka a adalah kelipatan bilangan bulat m atau a habis dibagi m.

IV. PERSAMAAN DIOPHANTINE

Persamaan Diophantine adalah persamaan yang semua koefisien dan penyelesaiannya bilangan bulat. Persamaan ini merupakan persamaan polinom dengan banyak peubah berbentuk:

$$f(x_i) = 0$$
atau
$$f(x_1,x_2,x_3,\ldots,x_n) = 0$$

dengan x_i lebih besar sama dengan 0 dan i=1,2,3,…,n. Persamaan ini memiliki koefisien dalam bentuk bilangan bulat yang akan dicari nilainya.

Persamaan Diophantine dibagi menjadi dua jenis yakni persamaan Diophantine linear dan persamaan Diophantine eksponensial. Persamaan Diophantine linear hanya menggunakan koefisien peubah berderajat satu. Sedangkan persamaan Diophantine eksponensial merupakan polinom berderajat lebih dari satu. Pada makalah ini hanya akan dibahan persamaan Diophantine linear yang memiliki bentuk dasar:

$$a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_nx_n = c$$

Persamaan ini adalah dasar dari pembuatan kunci dalam algoritma kriptografi nirsimetri dengan a sebagai kunci, x_i melambangkan bagian dari plainteks, serta c melambangkan bagian dari cipherteks. Penyelesaian dari persamaan Diophantine linear yang akan digunakan ini harus berupa bilangan bulat positif. Alasannya adalah pengkodean pesan menggunakan kode ASCII yang berupa bilangan bulat positif. Tidak ada kode ASCII yang bernilai negatif.

A. Teorema I

Terdapat $x_1, x_2, x_3,\ldots,x_n$ yang merupakan bilangan bulat sehingga memenuhi persamaan:

$$a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_nx_n = c,\ n>1$$

dengan a dan c merupakan bilangan bulat dan tidak bernilai 0. Persamaan dengan ketentuan di atas dapat dipenuhi jika dan hanya jika PBB $(a_1,a_2,a_3,\ldots,a_n)$ adalah faktor pembagi c agar penyelesaian berupa bilangan bulat.

Penyelesaian dapat dicari dengan menggunakan algoritma Euclidean. Misalkan terdapat persamaan sederhana:

$$35x+82y = 386$$

Pertama, cek PBB(35,82) apakah merupakan faktor pembagi c.

$$PBB(35,82) = 1$$

Nilai PBB adalah 1 yang adalah faktor pembagi 386 sehingga persamaan memiliki solusi bilangan bulat. Lalu digunakan algoritma Euclidean:

$$82 = 35 \cdot 2 + 12$$
$$35 = 12 \cdot 2 + 11$$
$$12 = 11 \cdot 1 + 1$$
$$11 = 1 \cdot 11 + 0$$

Dari hasil algoritma Euclidean, dilakukan pembalikan algoritma Euclidean:

$$1 = 12 \cdot 1 - 11 \cdot 1$$
$$1 = -35 \cdot 1 + 12 \cdot 3$$
$$1 = 82 \cdot 3 - 35 \cdot 7$$

Hasil pembalikan algoritma Euclidean dikalikan dengan 386, menjadi:

$$386 = 82 \cdot 1158 - 35 \cdot 2702$$

Maka solusi dari persamaan diophantine 35x + 82 y = 386 adalah

$$x = -2702 \text{ dan } y = 1158$$

Persamaan Diophantine linear dapat memiliki solusi lebih dari satu yang dibahas pada teorema II.

B. Teorema II

Pada persamaan linear, jika PBB $(a_1,a_2,a_3,\ldots,a_n)$ adalah faktor pembagi c, maka dapat dihasilkan solusi - solusi tak terbatas. Jika bentuk persamaan linear adalah ax + by = c, maka solusi tak terbatas memnuhi bentuk:

$$x = x_0 + \frac{b}{PBB(a,b)}t$$
$$y = y_0 - \frac{a}{PBB(a,b)}t$$

dengan x_o dan y_0 adalah sembarang solusi serta t adalah sembarang bilangan bulat.

Contoh persamaan linear 35x+82y = 386 pada teorema I yang memiliki solusi x = -2702 dan y = 1158. Solusi tersebut tidak dapat digunakan dalam sistem kriptografi kunci publik karena terdapat solusi berupa bilangan bulat negatif. Untuk itu perlu dicari solusi lain agar x dan y keduanya berupa bilangan bulat positif.

Dengan nilai x_0 = -2702, y_0 = 1158, a = 35, dan b = 82, dicari bilangan bulat t agar menghasilkan x dan y positif. Nilai PBB(35,82) sudah didapatkan sebelumnya, yakni 1. Contoh nilai t yang memenuhi adalah 33. Sesuai dengan teorema II, solusi didapatkan dengan:

$$x = -2702 + \frac{82}{1}.33$$
$$y = 1158 - \frac{35}{1}.33$$

Sehingga didapatkan

$$x = 4 \text{ dan } y = 3$$

yang adalah bilangan bulat positif.

V. PERSAMAAN DIOPHANTINE PADA KRIPTOGRAFI

Dasar matematis dan perhitungan matematis kriptografi kunci publik sebagai berikut:

$$z = ax + by$$
$$cz = acx + bcy$$

Bila ac = 1 mod d dan bc = e mod d, maka x = cz mod d mod e. Menurut jurnal *A New Public-Key Cipher System Based Upon the Diophantine Equations* dasar matematika pembentukan sistem kriptografi adalah sebagai berikut.

Misalkan w bilangan bulat positif dan domain D himpunan bilangan bulat positif pada [0,w]. Misalkan $w = 2^b-1$dengan b adalah bilangan bulat positif. Pesan yang akan dienkripsi panjangnnnya nb bit dipecah menjadi n buah b bit yang dinamakan $m_1,m_2,\ldots,m_n$.

Selanjutnya ditentukan pasangan bilangan bulat $(q_1,k_1),(q_2,k_2),\ldots,(q_n,k_n)$ dengan syarat-syarat:

1. q_i dan q_j relatif prima; PBB$(q_i,q_j)=1$ dengan $i \neq j$
2. $k_i > w$ untuk i = 1,2,…,n
3. $q_i > k_i$ $w(q_i \bmod k_i)$, dan $q_i \bmod k_i \neq 0$, untuk i = 1,2,…,n

Pasangan-pasangan (q_i,k_i) yang sudah memenuhi syarat akan digunakan sebagai kunci privat dan harus dirahasiakan. Karena akan digunakan untuk dekripsi pesan, maka kondisi di atas dinamakan kondisi DK.

Selanjutnya dilakukan penghitungan - penghitungan sebagai berikut. Pertama dihitung $R_i = q_i \bmod k_i$. Lalu dihitung pula P_i yang memenuhi dua buah kondisi:

1. $P_i \bmod q_i = R_i$
2. $P_j \bmod q_i = 0$ jika $i \neq j$

Dikarenakan qi relatif prima satu sama lain, solusi untuk P_i yang memenuhi kondisi-kondisi di atas adalah $P_i = Q_ib_i$ dengan Q_i adalah:

$$Q_i = \prod_{j \neq i} q_i$$

dan b_i harus memenuhi $Q_ib_i \bmod q_i = R_i$. Selanjutnya dihitung

$$N_i = \lceil q_i/(k_iR_i) \rceil$$

dengan i =1,2,…,n. Terakhir dihitung nilai:

$$s_i = P_iN_i \bmod Q$$

dengan nilai Q:

$$Q = \prod_{i=1}^{n} q_j$$

Didapat vector $S = (s_1,s_2,s_3,\ldots,s_n)$. S digunakan untuk melakukan enkripsi dengan melakukan perkalian cross antara $M = (m_1,m_2,\ldots,m_n)$ dan $S = (s_i,s_2,\ldots,s_n)$:

$$C = M*N$$

dengan C adalah chiperteks.

VI. KEAMANAN ALGORITMA KRIPTOGRAFI

Algoritma kriptografi harus dianalisis kekuatannya terhadap serangan-serangan yang mungkin dilakukan oleh para kriptanalis. Tiga serangan yang dapat dilakukan kriptanalis antara lain *brute force* untuk mendekripsi cipherteks, berusaha mendapatkan kunci dekripsi, dan menggunakan PBB kunci enkripsi.

A. Brute Force untuk Mendekripsi Cipherteks

Pada serangan ini, kriptanalis dimisalkan sudah mendapatkan cipherteks dan kunci enkripsi. Lalu kriptanalis akan memaksa mencoba mendekripsi cipherteks yang telah didapatkan dengan bantuan kunci enkripsi untuk menemukan algoritma kriptografi yang digunakan. Hal ini tidak mudah digunakan karena dibutuhkannya kepahaman secara mendalam mengenai teori bilangan *NP-complete* serta *Integer Knapsack.* Setelah memahami materi tersebut masih diperlukan pengambilan data untuk mengetes dengan jumlah yang banyak serta komputer yang memiliki tingkat paralelisme yang tinggi. Sehingga sesuai dengan kekuatan algoritma kriptografi yang telah dibahas sebelumnya, Algoritma ini baik menurut kompleksitas data dan kebutuhan memori.

B. Mendapatkan Kunci Dekripsi

Pada serangan ini kriptanalis dimisalkan sudah mendapatkan beberapa kunci publik. Lalu kriptanalis berusaha menemukan kunci privat. Hal ini sulit dilakukan karena kriptanlis kembali harus mengetahui dan mengerti algoritma kriptografi yang digunakan untuk pembuatan kunci. Pasangan-pasangan kunci dekripsi yang didapatkan kriptanalis belum tentu dapat memenuhi kondisi DK pada bab sebelumnya sehingga lagi-lagi diperlukan data yang banyak untuk mendapatkan kunci dekripsi. Sesuai dengan konsep komplkesitas data, algoritma ini termasuk algoritma baik.

C. Menggunakan PBB Kunci Enkripsi

Pada serangan ini, kriptanalis diasumsikan sudah mendapatkan kunci publik dan cipherteks. Kompleksitas algoritma ini sangat besar sehingga memerlukan waktu yang sangat lama dan mencapai bertahun-tahun. Oleh karena itu algoritma ini tergolong algoritma yang baik berdasarkan Kompleksitas Proses.

VII. KESIMPULAN

Kriptografi sangat dibutuhkan pada sistem komputer untuk melindungi data dan hak pihak yang berwenang atas data tersebut. Salah satu cara pengamanan data menggunakan algoritma kriptografi yang menggunakan persamaan Diophantine yaitu algoritma yang menerapkan sistem kriptografi nirsimetri. Algoritma ini dinilai cukup kuat berdasarkan kompleksitas data, kompleksitas proses, dan kebutuhan memori untuk menerobosnya.

VIII. UCAPAN TERIMA KASIH

Pertama-tama penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas terbentuknya makalah ini. Tanpa

kuasa-Nya, maka niscaya penulis tidak akan dapat menyelesaikan seluruh proses pembuatan makalah ini.

Penulis juga berterima kasih kepada dosen pembimbing kami, Dr. Ir. Rinaldi Munir, MT. karena telah membantu penulis menyelesaikan makalah ini, dengan pembekalan materi.

Adapun makalah yang penulis buat ini masih jauh dari sempurna, oleh karena itu kami mohon maaf jika ada salah pengucapan maupun salah penyusunan kata.

Penulis akan merasa sangat tersanjung jika saudara/i bersedia untuk memberikan kritik maupun saran. Kritik dan saran itu nantinya akan menjadi masukan tersendiri bagi kami untuk menyempurnakan makalah berikutnya.

Akhir kata, penulis mengucapkan terima kasih dan semoga makalah ini akan berguna bagi kita semua.

REFERENSI

[1] C.H.Lin, C.C.Chang,dan R.C.T. Lee.1995.A New Public-Key Cipher System Based Upon the Diophantine Equations.IEEE TRANSACTIONS ON COMPUTERS.44(1) pp. 14-15.

[2] Herry Sutarno.2007. ENKRIPSI DATA SISTEM KRIPTOGRAFI KUNCI PUBLIK MENGGUNAKAN ALGORITMA DIOPHANTINE. Jurnal Pengajaran MIPA.10(2) pp. 14–20.

[3] Munir,Rinaldi.2009.Matematika Diskrit, Bandung: Informatika Bandung,.

[4] Shinya Okumura.2015. A Public Key Cryptosystem Based on Diophantine Equations of Degree Increasing. Type.*Pacific Journal ofMathematics for Industry.7(4).*

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, 3 Desember 2018

Lydia Astrella Wiguna
13517019