Algoritma Kriptografi Kunci Publik pada Grup Selain Elliptic Curve Group

Kinantan Arya Bagaspati / 13519044
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13519044@std.stei.itb.ac.id

***Abstract*—Kriptografi sebagai salah satu bagian kritis dari bidang keilmuan teknologi informasi, khususnya dalam bidang keamanan hadir dalam berbagai bentuk dan jenisnya. Mulai dari fungsinya yang berkisar antara komunikasi searah, dua arah, maupun sekedar menjaga integritas pesan, atau dari algoritma yang digunakan yang sangat banyak jumlahnya seperti RSA, MD5, enigma, dan lainnya. Dua algoritma, yakni Elgamal dan ECC, dapat dilihat memiliki hubungan khusus yang dapat dijabarkan melalui bantuan bidang keilmuan lain yakni aljabar abstrak. Oleh karena itu, pengaplikasian keilmuan ini secara lebih lanjut dapat berpotensi menghasilkan algoritma baru yang sama atau bahkan lebih kuat dari algoritma pendahulunya.**

Keywords—Grup, Elgamal, Elliptic Curve

I. Latar Belakang

Kemanan Siber (CyberSecurity) merupakan topik yang hangat dibahas dalam era digitalisasi informasi ini. Dalam zaman di mana informasi dapat dengan sangat mudah didapatkan baik bila dilihat dari sudut pandang volume, varian, sumber yang berbeda, tujuan yang beragam, kategori, bentuk, format, dan lainnya, tentunya terdapat banyak sekali potensi masalah yang harus diatasi sebelum berubah dari resiko menjadi kerugian yang berdampak buruk pada sekelompok pihak. Topik ini memfokuskan pada permasalahan yang berkaitan dengan keamanan data (*data security*) yang sering disebut sebagai CIA triad.

Gambar 1. CIA Triad

Sumber: https://www.agus-hermanto.com/blog/detail/definisi-keamanan-informasi-3-aspek-di-dalamnya

CIA triad berupa *Confidentiality*, *Integrity*, dan *Availability*. Confidentiality merupakan aspek yang mengatur akses dari suatu data agar hanya diberikan pada pihak yang memiliki hak/peran untuk melihatnya. Integrity merupakan metode untuk memastikan data yang diterima memiliki nilai kredibilitas, benar terkonfirmasi sumbernya, dan terpercaya secara menyeluruh. Sedangkan availability merupakan aspek yang memastikan data dapat diakses atau terkirim dengan baik agar memiliki guna dalam masa hidupnya. Dalam makalah ini, bidang keilmuan yang dibahas yakni kriptografi utamanya menyinggung dua dari 3 aspek yakni confidentiality dan integrity.

Meskipun merupakan pengerucutan dari ilmu *cyber security* dan teknologi informasi secara umum, kriptografi sebenarnya masih sangat luas ranah cakupannya. Ilmu kriptografi yang menyinggung aspek integritas diantaranya hashing. Sementara ilmu yang menyinggung aspek confidentiality diantaranya Steganografi, kriptografi kunci simetris, dan kriptografi kunci asimetris. Namun meskipun tidak terlihat secara kasat mata, terdapat algoritma dalam kriptografi kunci asimetris yang lahir dari algoritma lainnya, dengan hubungan yang hanya bisa dijabarkan oleh Aljabar Abstrak.

Melalui fakta ini, makalah ini bertujuan mengeksplorasi potensi yang tak terbatas dari pengaplikasian Teori Grup dalam algoritma kriptografi yang sudah ada, guna kemudian dianalisa kelebihan yang diperoleh tentunya dengan fungsi yang sama yakni menjaga confidentiality. Algoritma yang akan diaplikasikan ini ialah Elgamal dan ECC, dengan grup yang merepresentasikannya yakni grup bilangan modulo prima dengan operasi perkalian dan grup kurva eliptik. Sedangkan grup yang akan dioperasikan ialah grup bilangan modulo prima dengan operasi penjumlahan, grup bilangan kompleks dengan operasi perkalian, grup transformasi kompleks dengan bentuk khusus dengan operasi komposisi, serta grup aritmatik dengan operasi dirichlet convolution.

II. Landasan Teori

A. Aljabar Abstrak

Aljabar Abstrak adalah salah satu bidang studi dalam ranah keilmuan matematika, yang mempelajari tentang Struktur

Aljabar. Struktur aljabar ialah sebuah sistem yang terdefinisi secara runtut dan jelas yang berlaku pada kumpulan elemen, yang biasa disebut himpunan yang mengikuti serangkaian axioma atau hal yang mengatur hubungan antar elemen dalam sistem tersebut. Struktur aljabar yang telah terdefinisikan dalam bidang keilmuan ini beragam jenisnya, serta studi yang dilakukan pada struktur-struktur ini didasarkan pada motivasi ilmuwan untuk men-*general*-kan axioma aljabar guna mentranslasikan operasi yang selama ini hanya diketahui pada ranah aljabar ke segala bentuk sistem yang dapat diamati.

Bila dianalogikan dalam bidang informatika, studi mengenai aljabar abstrak dirasa penulis sangat mendeskripsikan operator overloading pada Object Oriented Programming. Hal ini dapat dilihat dari definisi operator yang berlaku pada semua objek dalam satu kelas, serta kumpulan objek dalam satu kelas tentunya memiliki sifat sama yang dibawa dari lahir. Dengan mempertimbangkan hal ini, penulis hanya akan mengambil struktur aljabar yang relevan dalam kriptografi kunci publik, yakni grup dan medan.

Grup (Group, notasi: <G,*>) adalah struktur aljabar yang terdiri dari sebuah himpunan G, dan sebuah operasi biner (operasi yang mengasosiasikan tepat 2 elemen pada grup), dengan 4 sifat utama yakni:

- Klosur, yakni hasil dari a*b harus merupakan anggota dari G, bila a dan b merupakan anggota G.
- Asosiatif, yakni a*(b*c) = (a*b)*c. Sifat ini juga menyebabkan dapat dibuat definisi perkalian sebuah skalar bilangan asli m dengan a sebagai anggota G sehingga ma = a*a*….*a sebanyak m buah a, tanpa ada ambiguitas peletakan tanda kurung dalam perkaliannya.
- Elemen identitas e, yakni tepat satu anggota dari G yang memenuhi a*e = a untuk setiap a anggota G. Dengan kata lain e = 0a untuk setiap a anggota G. Mudah dibuktikan bahwa terdapat tepat satu identitas grup G dengan kontradiksi, yang bukan merupakan fokus makalah ini.
- Adanya invers dari tiap anggota G, yakni dinotasikan a’ sebagai invers dari a, yang memenuhi a*a’ = e. Dapat juga didefinisikan secara tidak ambigu bahwa a’ = (-1)a

Sebagai contoh dan diperlukan sebagai gambaran dalam segmen selanjutnya, dua grup yang relevan ialah:

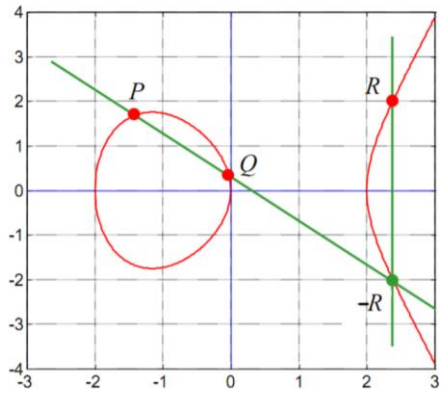
- <Z_p - {0}, x>, yakni himpunan semua bilangan dalam modulo prima p kecuali 0, yakni {1, …, p-1}, dengan operasi perkalian dalam modulo p. Mudah dibuktikan sifat grup terpenuhi seperti elemen identitas berupa 1 dan invers ada.
- Elliptic Curve Group dengan himpunan titik dalam koordinat kartesius yang memenuhi persamaan

$$y^2=x^3+ax+b$$

untuk suatu bilangan real a dan b yang memenuhi

$$4a^3 + 27b^2 \neq 0,$$

termasuk point of infinity, sebut saja P∞.



Gambar 2. Operasi penjumlahan pada kurva elips

Sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/ECC-2020-Bagian2.pdf

Operasi + pada grup ini yang berupa P * Q dengan P dan Q titik pada himpunan didefinisikan sebagai invers dari titik potong ketiga (selain P dan Q) dari garis PQ dan kurva elips. P∞ sebagai elemen identitas merupakan hasil penjumlahan elemen dengan inversnya, yakni bila divisualisasikan menjadi garis vertikal yang hanya memotong kurva pada tepat 2 titik.

Secara matematis, Apabila titik P berkoordinat (x_p,y_p) dan Q berkoordinat (x_q,y_q), maka koordinat (x_r,y_r) dari titik R = P+Q dapat dihitung dengan langkah berikut

$m = (y_p-y_q)/(x_p-x_q)$

$x_r = m^2-x_p-y_q$

$y_r = m(x_p-x_r)-y_p$

Beberapa grup juga dapat dikategorikan lagi karena memiliki sifat tambahan yang tidak wajib dimiliki grup, misalnya:

- Grup Abelian adalah grup dengan operasi yang komutatif,
- Grup Siklis adalah grup yang setiap anggotanya dapat dinyatakan dengan perkalian suatu skalar dengan tepat satu anggota grup, yang disebut sebagai generator,
- Grup Dihedral adalah grup yang memiliki lebih dari 1 elemen sebagai generator, dan lainnya

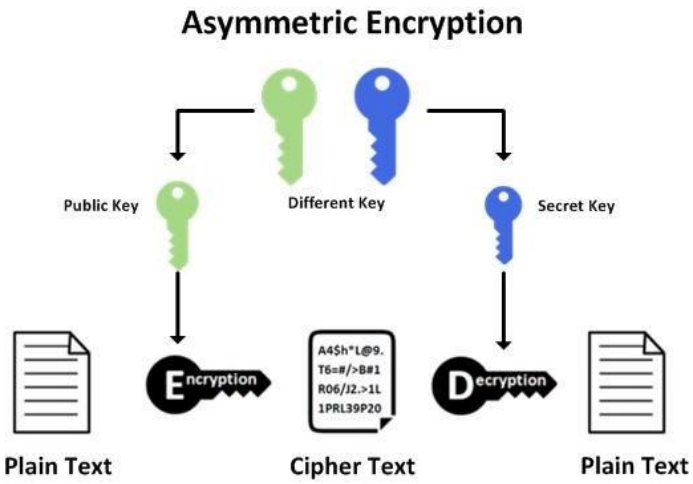
Medan (Field, notasi: <F,+,x>) adalah sebuah struktur aljabar dengan himpunan F dan dua operasi biner, sebutlah + dan x, yang memenuhi:

- <F,+> adalah grup abelian dengan identitas e_+
- <F-{e_+},x> adalah grup abelian juga dengan identitas e_x
- Distributif, yakni a x (b + c) = (a x b) + (a x c)

Perlu juga disinggung dalam makalah ini yakni medan galois (notasi: GF(p^n)) adalah medan berhingga yang jumlah anggota pada himpunannya senilai dengan pangkat suatu prima.

B. Algoritma Kriptografi Kunci Publik

Kriptografi adalah bidang keilmuan yang berfokus pada analisis dan riset mengenai metode-metode yang dingunakan untuk menjaga keamanan pesan bermakna. Metode yang diutamakan dalam keilmuan ini ialah metode yang mentransformasi pesan tersebut dengan sebuah algoritma dan kunci sedemikian sehingga sulit diterka maknanya oleh orang awam (enkripsi), selagi dapat diubah kembali ke bentuk awal oleh penerima (dekripsi). Metode lain menyembunyikan makna pesan dapat berupa metode penyisipan pesan dalam ojek lain sehingga tidak terlihat oleh mata awam, namun bidang keilmuan ini masuk ke dalam ranah steganografi yang tidak dibahas dalam makalah ini.



Gambar 3. Kriptografi Asimetris

Sumber: https://www.researchgate.net/figure/Asymmetric-encryption-primitive_fig2_321123382

Kriptografi menurut jenis kuncinya dibedakan menjadi simetris dan asimetriis. Kriptografi kunci publik, atau sering disebut juga sebagai kriptografi asimetris ialah algoritma yang membutuhkan kunci yang berbeda dalam metode enkripsi (kunci publik) dan dekripsi (kunci privat), berbeda dengan simetris yang bernilai sama. Hal ini menyebabkan kriptografi ini digunakan dalam komunikasi satu arah karena enkripsi dapat dilakukan secara publik asal mengetahui kunci publik, dan hanya pemilik kunci privat saja yang dapat mendekripsi isi pesan tersebut. Algoritma kunci publik yang relevan dalam makalah ini hanyalah algoritma elgamal dan Elyptic Curve Cryptography (ECC)

Dasar dari algoritma Elgamal ialah sulitnya menyelesaikan persamaan logaritma dalam modulo, yakni mencari solusi x dari persamaan

$$g^x \equiv y \pmod p$$

dalam kompleksitas waktu atau memori dibawah O(p). Algoritma ini dimulai dari bilangan prima p, kemudian dibangkitkan sebuah bilangan acak g dalam modulo p. Kunci rahasia berisi bilangan x, sedangkan bilangan p, g, dan y yang dihitung dari persamaan di atas dipublikkan, dengan dasar sulit dikalkulasi nilai x juga meski diketahui g, y, dan p.

Enkripsi elgamal dilakukan blok demi blok. Misalkan suatu blok bernilai m, maka dienkripsi menjadi sepasang bilangan $(g^k, y^k m)$ setelah dibangkitkan bilangan acak k antara 1 hingga p-2. Sementara dekripsi pasangan bilangan (Q,R) cukup dilakukan kalkulasi dengan memanfaatkan invers, identitas, dan perpangkatan yakni $Q^{-x}R$ pasti kembali menghasilkan m. Dengan kedua algoritma ini lengkap sudah definisi metode elgamal, serta cukup jelas bahwa cipherteks memiliki ukuran rata-rata 2 kali lipat dari plainteks, bagaimanapun versi implementasinya.

Bila kita melihat dari sudut pandang bahwa algoritma elgamal merupakan algoritma yang pengerjaannya dilakukan di atas grup pertama yang dicontohkan pada segmen landasan teori sebelumnya, yakni $<Z_p - \{0\}, x>$, cukup jelas bahwa elgamal didasari pada kesulitan penyelesaian persamaan yang mengandung perkalian skalar pada grup ini (pangkat dalam modulo merupakan perkalian elemen grup beroperasi perkalian dengan skalar), serta himpunan $Z_p - \{0\}$ juga cocok berdasarkan metode yang dijabarkan di atas. Oleh karena itu akan mempersingkat pembahasan bila dinyatakan bahwa sesungguhnya ECC didasari hal yang sama namun pada grup kedua yang dicontohkan, yakni Elliptic Curve Group.

ECC menggunakan algoritma enkripsi dan dekripsi yang serupa dengan elgamal, namun alih-alih beroperasi pada bilangan dalam modulo prima, ECC beroperasi pada titik dalam kurva suatu elips, yang agar dapat dinyatakan dalam bilangan bulat, dinyatakan dalam medan galois suatu prima juga. Oleh karena itu, ECC memiliki keunggulan tambahan yakni meski diketahui prima p yang digunakan, tetap sulit menemukan satu solusi saja dari persamaan modulo

$$y^2 = x^3 + ax + b \pmod p$$

Hal ini juga menambah sebuah permasalahan baru yang diimplemenkan dala berbagai versi juga, yakni pemetaan himpunan nilai blok yang mungkin ke dalam suatu titik dalam kurva. Contoh solusinya ialah membangkitkan 256 titik (asumsikan nilai ASCII saja yang perlu dipetakan) dengan mencari 1 titik, kemudian mengalikannya dengan 256 nilai skalar, atau menentukan 256 nilai x dengan selisih cukup berbeda, yang kemudian dicari nilai y yang memenuhi dengan menambah x satu per satu hingga ditemukan solusi. Kebanyakan versi tetap bersifat cipherteks berukuran rata-rata 4 kali lebih besar dari plainteks.

III. Algoritma Kriptografi Kunci Publik pada Grup Selain Elliptic Curve Group

Setelah mengetahui hubungan Elgamal dengan ECC, agar memudahkan pembahasan, mulai sekarang frasa ‘algoritma kunci privat/publik’ dalam makalah ini merujuk kepada algoritma enkripsi dan dekripsi layaknya algoritma elgamal yang telah dijabarkan pada landasan teori, namun tidak pada grup spesifik didefinisikan di atas, melainkan pada grup yang didefinisikan kemudian. Oleh karena itu, dapat didefinisikan enkripsi algoritma kunci publik pada grup $<G,*>$ adalah didasarkan pada sulitnya menemukan skalar x sehingga xg = y untuk suatu g dan y anggota G, yakni dengan memetakan anggota G berupa m ke pasangan anggota G (kg, ky*m), setelah dibangkitkan skalar acak k. Sedangkan dekripsi dari pasangan anggota G (a,b) ialah -xa*b.

Selanjutnya makalah ini akan membahas aplikasi kriptografi kunci publik/privat ini pada empat grup lainnya, terurut berdasarkan tingkat kompleksitasnya.

A. Grup Himpunan Zp dengan Operasi Penjumlahan dalam mod p

Grup ini merupakan grup paling sederhana yang akan dibahas dalam makalah ini. Zp dalam konteks ini adalah himpunan semua bilangan dalam modulo p. Operasi penjumlahan menandakan elemen identitas berupa 0, serta elemen invers dari a ialah (p-a). Dikarenakan kesederhanaannya, grup ini tidak memiliki keunggulan yang dimiliki elgamal, yakni sulitnya menerka jawaban xg = y untuk suatu g dan y anggota Zp, karena perkalian dengan skalar sesimpel perkalian modulo p saja. Sehingga mengingat Zp tidak hanya dapat diakomodir dengan grup namun dapat juga sebagai medan, operasi invers perkalian cukup trivial.

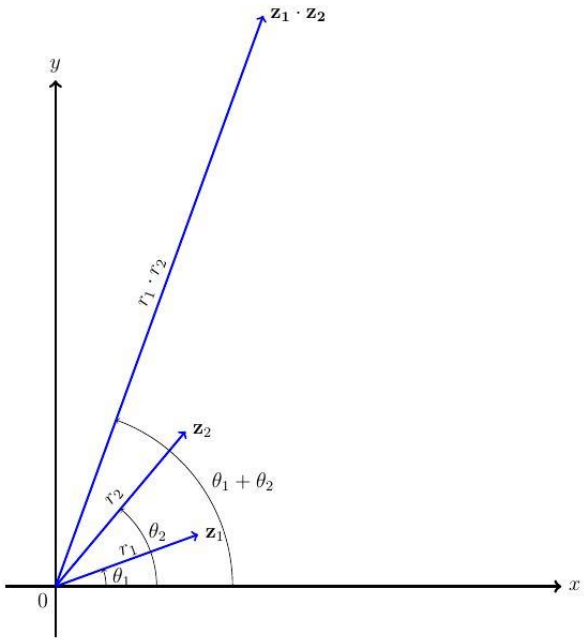
Analisis yang dilakukan dalam grup ini juga cukup singkat. Dilihat dari tingkat kesulitan pemecahannya yang rendah, grup ini hanya hadir dalam makalah ini sebagai dasar dan visualisasi/contoh apabila algoritma elgamal diaplikasikan pada grup yang trivial. Layaknya elgamal, cipherteks yang dihasilkan 2 kali lipat dari plainteks yang dihasilkan. Serta beda dengan ECC, tidak ada tantangan dalam memetakan karaker/simbol dalam pesan ke elemen dalam himpunan.

B. Grup Himpunan Cp dengan Operasi Perkalian Bilangan Kompleks

Himpunan bilangan kompleks merupakan kumpulan bilangan yang berbentuk (a+bi) dengan a dan b bernilai real dan i senilai dengan akar dari -1. Bilangan kompleks ini sering direpresentasikan dalam *complex plane* atau sebagai titik dengan koordinat (a,b) dalam koordinat kompleks dengan sumbu x memiliki unit 1 dan sumbu y memiliki unit i. Himpunan kompleks sendiri sesungguhnya dapat diakomodir dalam sebuah medan dengan operasi penjumlahan dan perkalian, Definisi penjumlahan sesungguhnya cukup intuitif, yakni dijumlahkan saja nilai koordinat masing-masing sumbu. Sedangkan nilai perkalian juga dapat dihitung sembari mengkonsiderasikan bahwa i^2=-1, yakni:

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

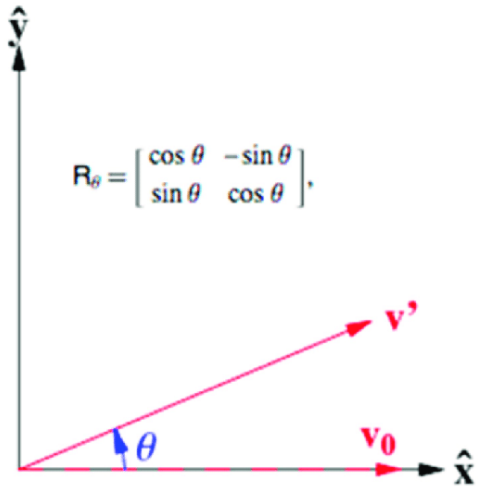
Tiap titik juga dapat didefinisikan melalui sistem koordinat yang lain yakni koordinat polar. Daripada mendefinisikan titik dalam sumbu x dan sumbu y, kedua titik kini mempunyai 2 properti yakni argument dan magnitude. Argumen ialah sudut dalam radian yang dibentuk oleh garis dari titik ke pusat, dengan garis sumbu x. Sementara magnitude, umumnya dinotasikan dalam |a|, merupakan panjang mutlak dari titik ke pusat koordinat. Sistem koordinat polar ini berguna karena hasil kali dari titik x dan y pasti memiliki argument jumlah dari argument x dan y, serta magnitude perkalian dari magnitude x dan y.



Gambar 4. Visualisasi erkalian bilangan kompleks pada koordinat polar

Sumber: https://socratic.org/questions/what-is-the-geometric-interpretation-of-multiplying-two-complex-numbers

Sifat dualitas inilah yang dapat digunakan dalam membuat operasi grup yang cukup kompleks guna dimanfaatkan dalam kriptografi asimetris ini. Alih-alih menggunakan koordinat polar, gunakanlah koordinat kompleks biasa dan dengan operasi perkalian, terjamin bahwa operasi gx = y sulit diterka nilai skalar x. Perhatikan pula bahwa grup ini merupakan homomorfisma dari grup dengan himpunan matriks 2x2 yang berbentuk matriks rotasi, dengan operasi perkalian matriks biasa. Homomorfisma merupakan bentuk kongruensi dari dua grup yakni terdapat pemetaan masing-masing elemen pada grup serta operasi yang digunakan. Ini menandakan potensi lanjutan implementasi untuk matriks 2x2 juga bisa dilakukan.



Gambar 5. Matriks Rotasi

Sumber: https://www.researchgate.net/figure/Rotation-of-data-using-a-rotation-matrix_fig2_334138261

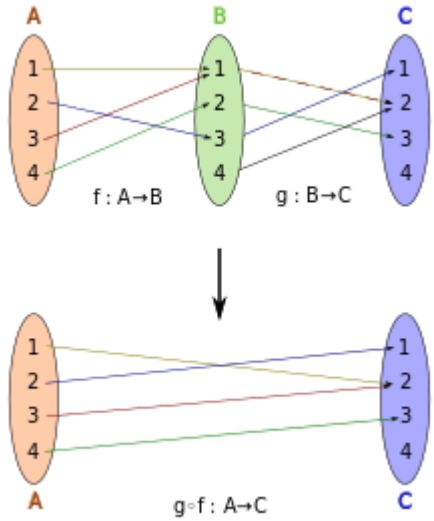
Dapat dimulai analisis grup ini dimata kriptografi asimetris. Agar dapat diaplikasikan, terutama dalam hal pemetaan simbol/karakter pada pesan ke elemen himpunan, tentunya akan jauh lebih mudah bila himpunan bilangan kompleks ini beralih dari koefisien real ke koefisien dalam bentuk field saja. Tentunya dinilai lebih mudah dari ECC, karena tiap titik lengkap masuk dalam himpunan. Di sisi panjang cipherteksnya, grup ini berpotensi menghasilkan 4 kalinya karena satu titik berisi 2 nilai. Sedangkan untuk matriks 2x2 tentunya dapat berukuran 8 kali lebih besar dari plainteks.

C. Grup Himpunan Fungsi Transformasi C ke C yang Berbentuk Tertentu dengan Operasi Komposisi Fungsi

` Bentuk yang dibahas dalam subbab ini adalah semua fungsi transformasi

$$z \mapsto \frac{az+b}{cz+d}$$

Untuk sejumlah bilangan real a, b, c, dan d sehingga ad-bc tidak sama dengan 0. Operasi komposisi fungsi sesuai definisinya ialah apabila fungsi f yang memetakan x ke y dilambangkan sebagai f(x) = y, maka fungsi f komposisi g memetakan x ke y dilambangkan sebagai (f o g)(x) = y = f(g(x)). Dengan kata lain pengaplikasian pemetaan fungsi f setelah dilakukan fungsi g.



Gambar 6. Komposisi fungsi

Sumber: https://en.wikipedia.org/wiki/Function_composition

Untuk sekilas, tentu saja sulit dipercaya bahwa struktur ini memiliki sifat klosur, yakni bahwa komposisi dari kedua fungsi dengan bentuk di atas juga menghasilkan fungsi baru dengan bentuk di atas juga, namun di sinilah letak salah satu keunggulan grup ini juga. Oleh karena itu, cukup dilakukan kalkulasi formula untuk mendapatkan nilai a, b, c, d dari hasil komposisi, maka diperoleh operasi yang sulit dipecahkan khususnya dari persamaan gx = y dengan x skalar.

Setelah dilakukan kalkulasi, dapat dilakukan observasi lebih lanjut bahwa ternyata ini merupakan faktor grup dari grup matrix 2x2 dengan operasi perkalian matriks biasa. Sama dengan segmen sebelumnya, tentunya diaplikasikan dulu medan modulo prima dalam representasi a,b,c,d untuk kemudahan transformasi. Ditambah lagi karena struktur yang sangat mirip dengan 2x2, yakni 4 nilai a,b,c,d untuk setiap titiknya, dengan pengecualian tertentu, yakni bila determinannya 0, grup ini tentunya dapat menghasilkan cipherteks berukuran 8 kali lipat dari plainteks.

D. Grup Himpunan Fungsi Aritmatik dengan Operasi Dirichlet Convolution.

Fungsi aritmatik adalah fungsi dengan domain bilangan asli dan kodomain medan apapun. Sedangkan konvolusi Dirichlet adalah suatu metode mengoperasikan 2 fungsi untuk menghasilkan fungsi baru dengan membawa sifat multiplikatif terhadap perkalian jika kedua nilai yang menjadi parameternya relatif prima. Dua fungsi f dan g dinyatakan berbeda apabila terdapat bilangan asli n sehingga f(n) tidak sama dengan g(n).

Setelah mendefinisikan himpunan fungsi ini, operasinya dari fungsi f dan g ialah

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Dengan fungsi identitas berupa:

$$\varepsilon(n) = \begin{cases} 1 & : \quad n = 1 \\ 0 & : \quad \text{otherwise} \end{cases}$$

Mudah dilihat berdasarkan identitas operasinya bahwa grup ini merupakan grup abelian.

Grup di atas merupakan contoh grup dengan himpunan yang unik dibandingkan dengan 3 grup yang telah dibahas sebelumnya. Karena masing masing elemennya merupakan pemetaan/fungsi yang tidak memiliki bentuk khusus, maka perlu metode tersendiri dalam memetakan karakter/simbol dalam pesan ke elemen grup ini. Salah satu metode yang terpikirkan ialah, asumsikan terdapat 256 jenis karakter yang mungkin, maka cukup diidentifikasi nilai n sehingga dapat dipetakan f(1) hingga f(n) kedalam sebuah nilai dalam field yang dipilih, yang tentunya untuk kemudapan dipilih modulo p. Dengan begini, tiap fungsi dapat dinyatakan dalam n bilangan antara 0 hingga p. Hal ini menyebabkan representasi yang dinamis, yakni ukuran cipherteks bisa diukur sebanyak 2n kali lipat lebih besar dari plainteks. Namun hal ini juga mempengaruhi kerumitan dirichlet convolution jika dibandingkan perkalian biasa jika n=1. Metode ini diharapkan menjadi contoh yang dapat diandalkan dalam melakukan pemetaan elemen teks ke dalam elemen grup yang berupa fungsi atau pemetaan.

IV. KESIMPULAN DAN SARAN

. Aljabar Abstrak merupakan bidang ilmu yang dapat dikaitkan dengan bidang seluas Teknologi Informatika, terutama yang dibahas dalam makalah ini, yakni ilmu kriptografi. Fakta bahwa adanya korelasi yang dapat diaplikasikan pada sepasang algoritma (Elgamal dan ECC) yakni kemiripan mendasar dari strukturnya, tentunya sangat sejalan dengan tujuan studi Aljabar Abstrak pada umumnya. Sekali lagi, tujuan Aljabar Abstrak ialah mengeneralisir sebuah sistem dengan mendefinisikan axioma axioma yang dapat

diturunkan untuk memvisualisasi properti tersembunyi yang tentunya berlaku dalam semua sistem yang memenuhinya. Dalam hal ini, algoritma kriptografi kunci publik yang dibahas ini tentunya dapat diaplikasikan hanya dengan mengganti struktur dimana algoritma ini dioperasikan.

Hal ini menyebabkan tumbuhnya potensi yang tidak terbatas. Di satu sisi, terdapat sangat banyak grup yang dapat diaplikasikan dalam algoritma kriptografi asimetris ini. Grup-grup ini tentunya harus memenuhi kriteria yang dibawa algoritma, dalam kasus ini berupa sulitnya menerka skalar x sehingga gx = y, serta tingkat kemudahan memetakan karakter/simbol pada pesan ke elemen dalam grup. Penulis berharap penelitian lebih lanjut dapat membuahkan hasil yang lebih mangkus menggunakan grup yang lebih kompleks namun indah, misalkan:

Di sisi lain, peluang juga dapat terbuka pada algoritma kriptografi selain Elgamal dan ECC, yang masih bekerja hanya pada struktur aljabar sederhana. Potensi modifikasi dapat dilakukan asalkan dapat secara sistematis dirumuskan kebutuhan struktur apa yang harus ada oleh algoritma ini. Korelasi selain Elgamal-ECC dari sudut pandang struktur aljabar juga bisa saja tidak

Pengaplikasian dua atau lebih bidang keilmuan sangat tidak jarang menghasilkan solusi yang kompleks namun dapat diaplikasikan. Metode ini memberikan sudut pandang yang majemuk dalam menyelesaikan persoalan.

V. Ucapan Terima Kasih

Pertama-tama, penulis mengucapkan terimakasih kepada puji syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmatnya, penulis bisa menyelesaikan tugas makalah ini. Penulis juga menguncapkan terimakasih kepada Bapak Rinaldi Munir selaku dosen mata kuliah Kriptografi, yang selama ini membimbing pembelajaran Kriptografi yang sangat membantu pengerjaan makalah ini, sekaligus menyediakan website yang dapat dengan mudah diakses berisi materi-materi kuliah, latihan-latihan soal untuk kuis dan ujian, dan semua dokumen pembelajaran, soal, dan lainnya yang tentunya berguna dalam proses pembelajaran Kriptografi.

References

[1] https://www.agus-hermanto.com/blog/detail/definisi-keamanan-informasi-3-aspek-di-dalamnya. Diakses pada 20 Desember 2021

[2] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/ECC-2020-Bagian2.pdf. Diakses pada 20 Desember 2021

[3] https://www.researchgate.net/figure/Asymmetric-encryption-primitive_fig2_321123382 Diakses pada 20 Desember 2021

[4] https://socratic.org/questions/what-is-the-geometric-interpretation-of-multiplying-two-complex-numbers. Diakses pada 20 Desember 2021

[5] https://www.researchgate.net/figure/Rotation-of-data-using-a-rotation-matrix_fig2_334138261 Diakses pada 20 Desember 2021

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, 20 Desember 2021

Kinantan Arya Bagaspati
13519044