Enkripsi Pesan dengan Metode Mirip List Sirkuler dan Bilangan Prima

Mico (13515126)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515126@std.stei.itb.ac.id

***Abstract*—Pada era yang serba digital ini, pengamanan pada suatu pesan ataupun data telah menjadi suatu kebutuhan primer. Ada banyak metode untuk melakukan enkripsi pada suatu pesan maupun data. Dalam pengamanan tersebut, akan sangat dibutuhkan algoritma unik sehingga keamanan dari pesan tersebut bisa dijamin. Dengan menggabungkan metode enkripsi dengan list rekursif, akan menambah keunikan algoritma yang ada.**

***Keywords*—Pesan, pengamanan, List rekursif.**

I. PENDAHULUAN

Semakin hari, pengetahuan dan perkembangan akan dunia teknologi yang ada semakin berkembang. Bahkan dapat dipastikan bahwa perkembangan teknologi yang ada ini tidak akan menemui titik henti untuk berkembang. Dikarenakan semakin berkembangnya teknologi, otomatis perkembangan data dan pengiriman data berupa pesan juga akan meningkat.

Semakin penting suatu informasi, maka semakin banyak pula pihak-pihak yang bukan pemilik informasi tersebut yang ingin memilikinya. Contohnya jika seseorang yang bernama A memiliki kode rahasia peluncuran nuklir Korea Utara, maka nilai dari informasi yang ada pada si A dianggap sangant mahal karena dapat mendatangkan hal-hal yang merugikan sekaligus menguntungkan. Seandainya A ingin mengirim informasi tersebut dalam bentuk pesan, maka A memerlukan suatu pengaman yang bisa menjamin hanya ia dan penerima informasi lah yang pantas melihat isi dari pesan tersebut.

Enkripsi bisa menjadi solusi dari masalah ini. Bahkan untuk semua pesan yang bersifat privasipun , enkripsi bisa menjadi pengaman yang menjamin bahwa informasi tersebut tidak akan bocor kepihak lain. Namun, untuk menemukan suatu algoritma enkripsi yang rumit dan sulit ditembus adalah perkara utama dari metode enkripsi ini. Algortima enkripsi yang dipakai harus susah ditebak ataupun dibongkar oleh pihak lain, karena itulah dibutuhkan seorang ahli enkripsi yang mampu merancang algoritma yang cukup rumit sehingga tingkat keamaan dari enkripsi itu dapat terjamin. Karena ketika algoritma enkripsi yang kita buat dapat ditebak atau dibongkar pihak lain, maka informasi yangpun akan jatuh kepihak lain.

II. DASAR TEORI

A.Enkripsi

Pada bidang Kriptografi,enkripsi adalah suatu proses untuk mengamankan suatu informasi dengan membuat informasi tersebut menjadi tidak dapat dibaca tanpa bantuan pengetahuan yang khusus. Pada awalnya, enkripsi hanya dipakai oleh kepentingan yang sangat-sangat mendesak dan tingkat kerahasiaan informasi tersebut sangatlah tinggi karena menyangkut masalah internal ataupun eksternal suatu negara. Namun karena bnyaknya metode yang dapat dipakai untuk proses enkripsi tersebut, maka saat ini enkripsi telah menyebar luas tidak terbatas hanya pada organisasi-organisasi yang besar saja, bahkan jaringan internet dan telepon yang adapun telah dienkripsi untuk membantu penduduk biasa mendapatkan hak privasi mereka.

Dalam enkripsi dikenal beberapa istilah :

1.*Ciphers*

Sebuah *chiper* adalah suatu algoritma untuk menampilkan enkripsi yang bertolak belakang dengan deskripsi.

2.*PlainText*

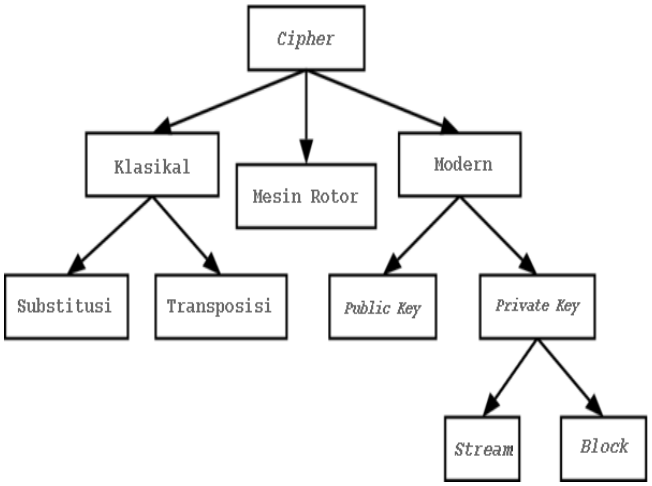
Sebuah *plaintext* berisi informasi asli yang belum mengalami enkripsi 1 kalipun.

3.*Superenchiperment*

Teknik yang menggabungkan code dan chipper untuk memaksimumkan tingkat keamanan pesan.

Tipe-Tipe Chipper

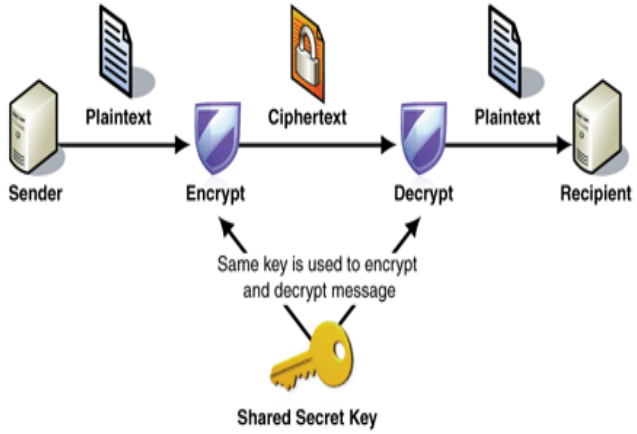
Ada banyak variasi dari tipe enkripsi yang berbeda, algoritma yang digunakan pada awal kriptografipun sudah banyak berbeda dengan metode modern, dan chipper modern diklasifikasikan berdasarkan bagaimana chipper tersebut bekerja dan apakah chipper tersebut memakai satu kunci atau dua dan lebih.



Tipe-Tipe *Chipper*

Metode enkripsi dibagi menjadi algoritma *symmetric key* dan *asymmetric key*. Pada *symmetric key*, pengirim dan penerima harus memiliki kunci yang digunakan bersama. Pengirim menggunakan untuk melakukan enkripsi, dan penerima menggunakan untuk melakukan deskripsi. Pada *assymetric key* terdapat dua kunci terpisah, sebuah *public key* diterbitkan dan membolehkan siapapun melakukan enkripsi, sedangkan sebuah *private key* dijaga kerahasiaannya oleh penerima dan digunakan untuk melakukan deskripsi.

Algoritma *symmetric key*, metode ini awalnya dipakai oleh Caesar, tekniknya adalah setiap huruf alphabet yang ada pada *plaintext*, digeser sebanyak 3 karakter ke kanan.



Ilustrasi Algoritma *symmetric key*

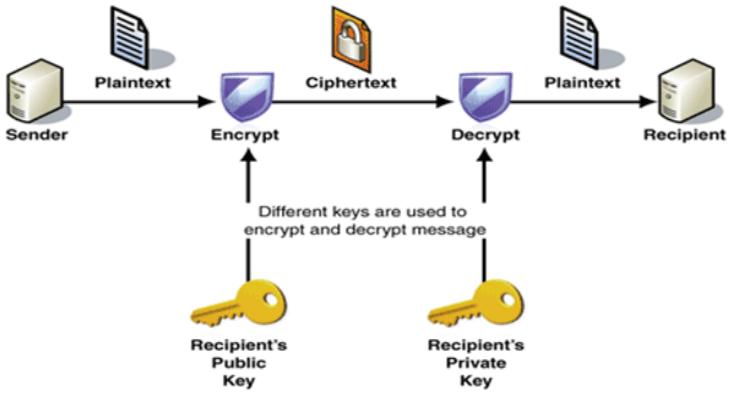
Algoritma *asymmetric key* memiliki langkah-langkah yang cukup unik , yaitu :

-Setiap pengguna memiliki sepasang kunci :

1.Kunci Publik, e :untuk enkripsi pesan

2.Kunci privat, p :untuk deskripsi pesan

-Kunci public tidak dirahasiakan



Ilustrasi Algoritma *symmetric key*

Algoritma pembangkitan pasangan kunci :

1.Pilih dua bilangan prima, p dan q dirahasiakan.

2.Hitung n=p*q. Besaran n tidak perlu dirahasiakan.

3.Hitung m=(p-1)*(q-1).

4.Pilih sebuah bilangan bulat untuk kunci public, e, relatif prima terhadap m.

5.Hitung kunci deskripsi ,d ,melalui kekongruengan e*d=1 mod m.

Enkripsi**:** $c_i = p_i^e$ **mod** n

Dekripsi**:** $p_i = c_i^d$ **mod** n

Pembangkit Bilangan Acak (*Random Number Generator*)

Pada zaman dulu, digunakan dadu ataupun mengocok kartu untuk mendapatkan angka acak. Namun, seiring perkembangan zaman, digunakan Pembangkit Bilangan Acak dengan basis yang berbeda-beda.

Misalnya untuk basis *linear congruential generator* :

$\boldsymbol{X_n = (aX_{n-1} + b) \bmod m}$

X_n = bilangan acak ke-n dari deretnya

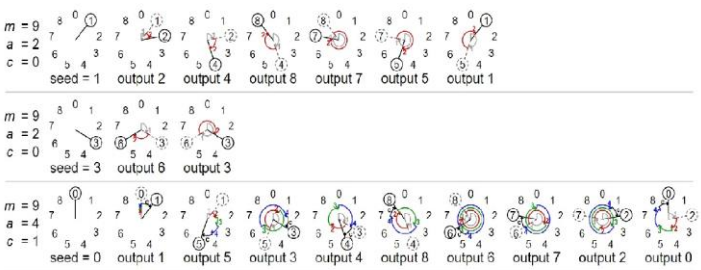
X_{n-1} = bilangan acak sebelumnya

a = faktor pengali

b = *increment*

m = modulus

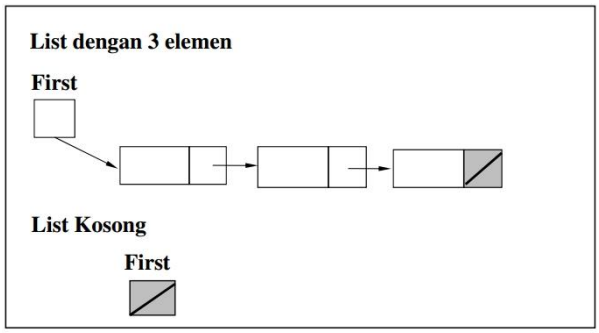
Kunci pembangkit adalah X_0 yang disebut **umpan** (*seed*).



Ilustrasi RNG dengan basis LCG

B.List Linier

Sebuah List Linier memiliki ciri:
1.Elemen pertama list, biasanya melalui alamat elemen pertama yang disebut :First.
2.Alamat elemen berikutnya sebagai suksesor, jika kita mengetahui alamt sebuah elemen, dapat diakses melalui informasi Next.
3.Setiap element memiliki alamat, yaitu elemen yang disimpan dapat diacu.
4.Elemen terakhirnya.

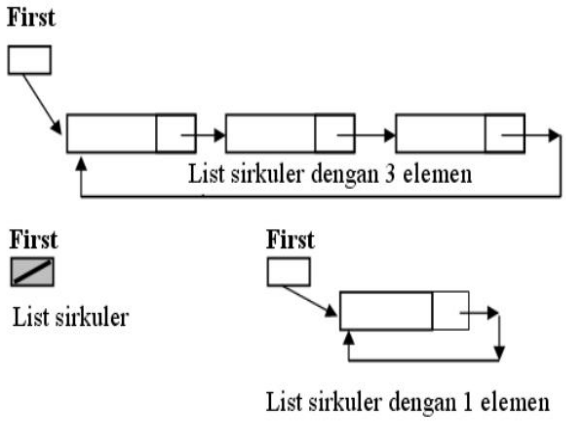


Ilustrasi List

Pada dasarnya untuk memproses suatu list, maka akan dikunjungi alamt dari tiap-tiap element list untuk diproses, sampai ditemukan element list yang terakhir.

C.List Sirkuler

Pada dasarnya, list sirkuler memiliki kesamaan yang persis dengan List Linier biasa, perbedaanya hanyalah bahwa seolah-olah List Sirkuler tidak memiliki elemen terakhir, hal ini dikarenakan akhir dari list linier di sambungkan ke elemen pertama dari list tersebut, sehingga elemen terakhir dari list seolah-olah ditiadakan.



D.Bilangan Prima

Sebuah bilangan dikatakan prima, jika dan hanya jika kofaktor dari bilangan itu adalah satu dan bilangan itu sendiri. Contoh : 2,3,5,7,11,13,dst.
Bilangan prima karena keistimewaannya yaitu tidak dapat diubah bentuknya menjadi kombinasi bilangan-bilangan lain. Seperti 18 yang bisa diuraikan menjadi 2x9, atau 3x6. Bilangan prima hanya memiliki 1 bentuk, misalnya 13 hanya dapat dibentuk dari 1 x 13.

Di alam, salah satu fenomena yang melibatkan bilangan prima ialah dalam kehidupan serangga spesies jengkerik yang bernama cicadas. Serangga ini menghabiskan sebagian besar waktunya sebagai larva di bawah tanah. Mereka hanya muncul dari tempat persembunyiannya setelah 13 atau 17 tahun. Di luar tempat persembunyiannya itu, mereka beterbangan, berkembang biak dan mati hanya selama beberapa minggu. Selang kemunculan serangga ini yang sekian lama dan berbasiskan bilangan prima diduga merupakan strategi bertahan hidupnya sehingga sulit bagi pemangsa-pemangsa untuk menjadi pemangsa mereka. Jika serangga cicadas muncul pada selang waktu non-bilangan prima, misalkan saja setiap 12 tahun, maka pemangsa-pemangsa yang berkembang biak setiap 2, 3, 4, 6 atau 12 tahun tentu akan bisa memangsanya. Dengan muncul setiap selang waktu bilangan prima, serangga cicadas lebih punya kesempatan bertahan hidup karena siklus kehidupannya sulit untuk dibarengi oleh siklus kehidupan pemangsa-pemangsanya.

Dalam aktivitas persandian mutakhir, hal tersebut tidak harus dilakukan. Logikanya sekarang dipermudah. Kedua belah pihak tak harus saling bertemu dan tak harus ada kurir. Proses meminta kita memasukkan kode saat kita hendak membuka akun email baru atau saat kita mengunduh suatu file di dunia maya memberikan kepada kita gambaran kongkret mengenai bagaimana logika persandian mutakhir. Mari kita pahami secara lebih sederhana apa yang terjadi dalam proses di dunia maya tersebut.
Misalkan kita ingin mengunduh suatu file. Misalkan saja kita telah masuk ke situs penyedia file yang kita butuhkan. Itu artinya kita telah bertemu dengan pihak pemilik informasi atau data.
Kemudian kita mengklik perintah mengunduh file. Itu sama artinya dengan kita mengajukan permintaan untuk mendapatkan informasi atau data yang dimiliki oleh pihak penyedia.
Setelah mengklik perintah mengunduh, kita mendapatkan perintah untuk memasukkan kode persis seperti yang ditunjukkan oleh pihak penyedia kepada kita. Itu artinya:
– yang pertama, pihak penyedia mengirimkan kunci yang bersifat khusus kepada kita dalam bentuk kode. Sifat khusus dari kode tersebut memiliki arti bahwa kode tersebut hanya ditujukan kepada kita dan bukan kepada yang lain. Dengan kata lain, pihak yang lain ditutup aksesnya oleh pihak penyedia.
– yang kedua, kita harus mengirimkan kembali kunci khusus itu kepada pihak penyedia sebagai jawaban bahwa kita sebagai pihak khusus yang dituju oleh pihak penyedia

telah menerima kunci tersebut. Dengan kata lain, pihak lain yang tak memiliki kunci khusus tersebut tak mungkin bisa memberikan jawaban kepada pihak penyedia dan tak mungkin melangkah ke tahapan selanjutnya.
Setelah menerima kembali kunci khusus yang kita kirimkan secara benar, barulah pihak penyedia memberikan informasi atau data seperti yang kita minta. Proses inilah yang merupakan manifestasi dari logika dunia persandian mutakhir. Perhatikan bahwa informasi atau data itu sesungguhnya telah ada di dalam situs sang pemilik informasi atau data (atau di dunia publik), hanya saja tidak semua pihak bisa mengaksesnya.

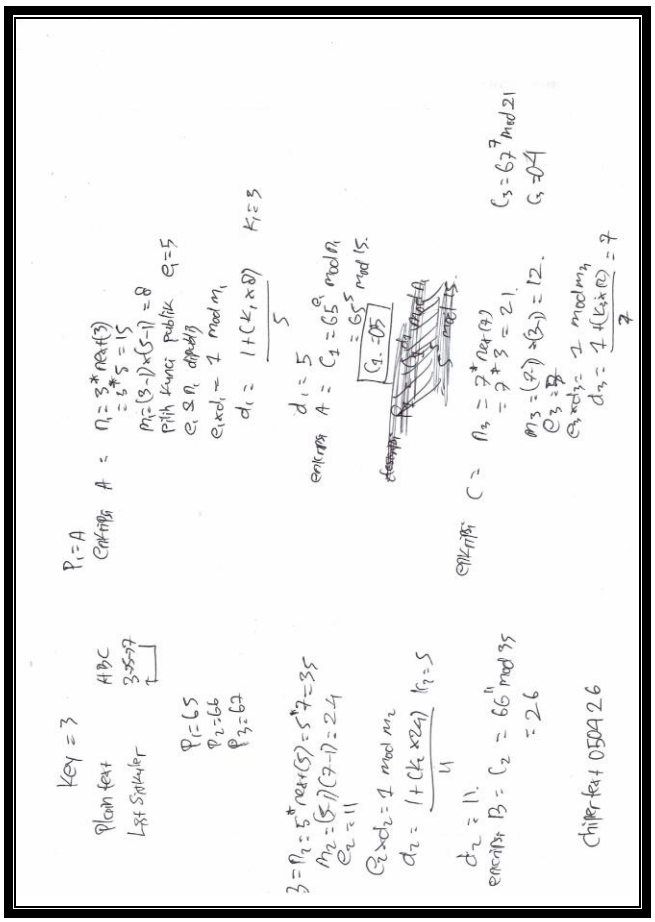
III. IMPLEMENTASI LIST SIRKULER DALAM ENKRIPSI PESAN

Sesuai dengan metode enkripsi, kita gunakan bilangan prima sebagai acuan untuk menggeser karakter pada pesan di *plaintext*. Perbedaan metode ini, adalah bilangan prima yang diberikan oleh pemilik pesan hanya satu bilangan prima. Namun, dalam prosesnya, kita pakai lebih dari 1 bilangan prima.

Prosedurnya adalah sebagai berikut:

1.Pemilik pesan men-*set* 1 bilangan prima, misalnya q.
2.q kita jadikan *first* elemen pada list sirkuler.
3.Bilangan prima yang menjadi *key* dari pemilik pesan, menjadi *key* untuk karakter pertama dari pesan.
4.*Key* untuk karakter selanjutnya, adalah bilangan prima setelah bilangan prima yang pertama, sekaligus menjadi elemen kedua dari list sirkuler yang ada.
5.Proses enkripsi yang terjadi adalah seperti pada gambar disamping.
Sehingga public key yang ada akan lebih dari 1. Dan penerima hanya perlu memiliki key saja , yaitu 3.

Kelebihan dari algoritma diatas adalah karena beragamnya bilangan prima yang dipakai dalam proses enkripsi, sehingga tingkat keamanan dari pesan tersebut bisa dijamin.



IV. CONTOH PERSOALAN

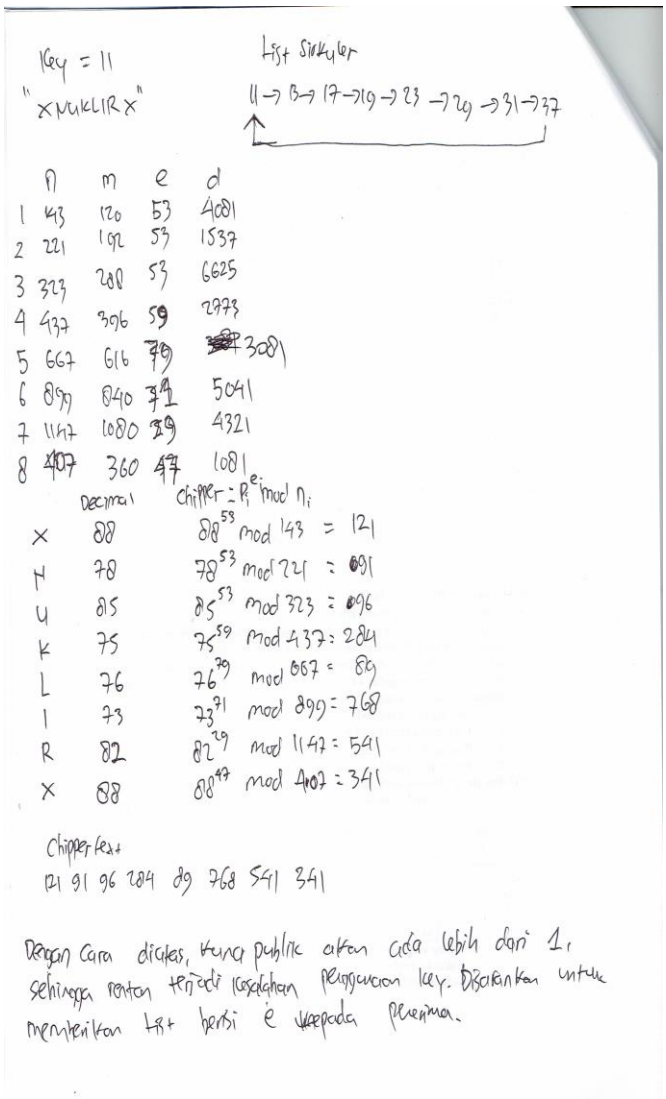
Pada saat konflik antar benua, beberapa negara maju khawatir kalau kode peluncuran mereka akan di sabotase oleh negara lain dan dapat menyebabkan pecahnya perang nuklir.

Untuk mencegah hal tersebut, maka pihak negara X berencana mengirim kode mereka ke brankas data yang berada di Paris untuk disimpan selamanya. Karena situasi yang masih panas dan rawan, maka pengiriman kode nuklir tersebut tidak dapat dilakukan secara fisik, tetapi harus dikirim melalui internet.

Bantulah agar negara X dapat mengirim kode nuklir mereka dengan bebas jika diberikan *plaintext* berikut ini:

"XNUKLIRX"

Penyelesaian:
Kita berikan Key =11.
Maka proses enkripsi yang terjadi adalah:



V. SIMPULAN

Penggabungan dari List Sirkuler pada enkripsi akan semakin meningkatkan tingkat keamanan data yang akan dikirim sehingga dapat dijamin bahwa pesan yang ada di dalamnya tidak akan ketahuan oleh pihak lain. Contoh pengaplikasian algoritma di atas tidak terbatas. Dengan adanya algoritma ini, diharapkan tingkat keamanan dalam enkripsi bisa lebih diperbarui.

VI. UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa, karena berkat rahmat-Nya lah makalah "Matematika Diskrit" ini dapat diselesaikan. Terima kasih kepada Bapak Rinaldi Munir dan Ibu Harlili selaku dosen pengajar mata kuliah "Matematika Diskrit", yang telah memberikan dan membagikan pengetahuan, khususnya dalam hal kriptografi. Terima kasih kepada Bapak Saiful selaku dosen mata kuliah "Algoritma dan Struktur Data" yang telah mengajarkan materi mengenai list.

DAFTAR PUSTAKA

[1] https://msdn.microsoft.com/en-us/library/ff650720.aspx diakses 8 Desember 2016.
[2] https://id.wikipedia.org/wiki/Enkripsi diakses 8 Desember 2016.
[3] https://en.wikipedia.org/wiki/Linear_congruential_generator diakses 9 Desember 2016.
[4] https://mengertimatematika.wordpress.com/2012/07/22/apa-hebatnya-bilangan-prima/ diakses 9 Desember 2016.
[5] www.wolframalpha.com diakses 9 Desember 2016.
[6] Munir, Rinaldi, Matematika Diskrit. Bandung: Percetakkan ITB, 2006, bab 5.

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, 8 Desember 2016

Mico/13515126