Kriptografi Unsur Kimia dalam Tabel Periodik

Lukman Hakim (13511004)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
lukman.hakim@students.itb.ac.id

Abstract

Makalah ini membahas tentang teknik kriptografi unsur kimia dalam tabel periodik. Tabel periodik terdiri atas 118 unsur dapat digunakan sebagai chiperteks dalam suatu plainteks menggunakan algoritma enkripsi tertentu. Hal ini merupakan hal yang baru digunakan. Penggunaan unsur kimia didasarkan pada banyaknya jumlah unsur kimia yang disertai sifat keperiodikannya sehingga dapat dijadikan sebuah kode dalam menyimpan sebuah pesan. Selain itu, bentuk tabel periodik yang unik juga membuat algoritma ini terlihat berbeda dari yang lain.

Algoritma ini dapat dikembangkan lebih lanjut sehingga menghasilkan sebuah algoritma yang kuat dan menjadi alternatif baru dalam kriptografi suatu pesan rahasia.

1 Pendahuluan

Pada saat ini, era globalisasi yang terus berkembang hal ini menjadikan media informasi menjadi sangat luas berperan. Segala informasi dapat kita peroleh darimana pun, dari informasi dalam negeri maupun mancanegara. Namun, tak semua informasi harus disebar dan diketahui orang lain bahkan ada informasi yang hanya boleh diketahui oleh orang-orang tertentu bahkan diri sendiri. Tak diragukan lagi, bahwa kerahasiaan informasi menjadi sangat penting, sehingga teknik kriptografi dalam penyandian pesan menjadi sangat penting.

Banyak algoritma kriptografi yang digunakan dalam penyandian pesan, sampai saat ini manusia masih terus mencari algoritma yang dapat membuat pesan rahasia namun hanya menggunakan sandi yang pendek. Saat ini, kriptografi yang populer digunakan adalah kriptografi RSA. kriptografi ini dipercaya mampu merahasiakan sebuah pesan sehingga dibutuhkan waktu 4 miliar tahun bagi sebuah komputer super cepat untuk memecahkanya. Namun, salah satu kerugian dari kriptografi ini adalah jumlah sandi yang digunakan terlalu banyak, bayangkan saja kita butuh 2 buah bilangan prima 200 digit untuk membuat sandi ini.

Bagi seseorang yang berkecimpung di bidang kimia, tabel priodik menjadi hal yang biasa dalam kehidupan mereka. Bahkan tabel periodik menjadi sebuah hal yang harus ada dalam setiap ruangan yang digunakan untuk mendalami ilmu kimia baik itu laboratorium kimia, ruang kelas, bahkan soal ujian kimia pun disertakan tabel periodik. Ternyata, tabel periodik juga berfungsi sebagai penyandi pesan sehingga tabel periodik juga dapat digunakan orang yang berkecimpung di bidang Teknik Informatika sebagai teknik dalam kriptografi.

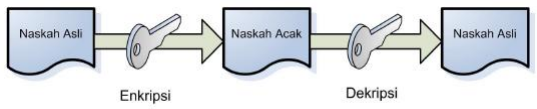
1.1 Kriptografi

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara menyamarkan (*to crypt* artinya menyamar) mempunyai bentuk tersandi yang tak memiliki makna[3].

Konsep dasar kriptografi adalah dengan merubah teks asli yang biasa disebut sebagai **plainteks** menjadi teks acak yang disebut sebagai **chi-**

perteks menggunakan algoritma tertentu. Proses ini disebut sebagai proses **enkripsi**. Selanjutnya, chiperteks dirubah kembali menjadi plainteks dengan algoritma tertentu, yang disebut sebagai proses **deskripsi**[2].

Dalam notasi matematika dapat ditulis :



Gambar 1: Proses Kriptografi

Proses enkripsi plainteks

$$E(P) = C \tag{1}$$

Proses deskripsi chiperteks

$$D(C) = P \tag{2}$$

Keseluruhan proses kriptografi

$$D(E(P)) = P \tag{3}$$

Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif di- bandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan- bilangan yang sangat besar. Namun, walaupun enkripsi asimetris lebih ma- hal dibandingkan enkripsi simetris, *public key cryptography* sangat berguna untuk *key management* dan *digital signature*[2].

Menurut sejarah, kriptografi sudah lama digunakan oleh tentara sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang disebut *scytale*. Alat ini terdiri dari sebuah pita panjang dari daun papyrus yang dililitkan pada sebuah batang silinder. Pesan yang dikirim ditulis horizontal. Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun membentuk pesan rahasia[3].

Saat ini, kriptografi telah digunakan secara luas dalam penyandian sebuah pesan. Algoritma yang digunakan pun beragam mulai dari yang paling sederhana hingga yang paling rumit. Bahkan, saat ini algoritma dari sebuah kriptografi sudah diseberkan secara luas sehingga semua orang mengetahui algoritma tersebut. Oleh karena itu, kriptografi seperti ini tidak mengandalkan kekuatan algoritma dalam poses enkripsi dan deskripsi tetapi mengandalkan penggunaan digit angka yang besar dan sulit untuk terpecahkan baik oleh manusia dan komputer super cepat. Contoh kriptografi seperti ini adalah kriptografi RSA yang menggunakan 2 buah bilangan prima 200 digit.

Dalam sebuah kriptografi kesulitan dalam pemecahan sandi menjadi hal yang utama. Semakin sulit suatu sandi dipecahkan, maka semakin baik teknik kriptografi yang digunakan. Namun, keunikan dari kriptografi tidaklah hanya sebagai sebuah ilmu pengetahuan melainkan sebuah seni yang digunakan untuk menyandikan sebuah pesan. Terkadang orang lebih tertarik terhadap pembuatan chiperteks yang unik dibandingkan dengan sebuah keamanan dari kriptografi sendiri, sebab ketika suatu kode sudah unik, maka penyelesaian kode itu pun akan semakin rumit disebabkan jarang orang yang melihatnya. Sehingga menjadi seorang **kriptografer**[1], tidak hanya memikirkan tentang kerumitan sebuah algoritma tetapi juga memikirkan bagaimana chiperteks yang dihasilkan unik dan membuat orang yang lain yang membacanya tak menyadari bahwa itu merupakan sebuah sandi rahasia.

Dalam kriptografi, ada yang disebut sebagai *cryptoanalyst*. Kriptoanalisis merupakan teknik dalam pemecahan kriptografi. Dalam melakukan kriptoanalisis ada tahapan tertentu yang harus dilakukan, yakni :

- *Known Plaintext Attack*
  Hal ini merupakan sebuah pengetahuan menganai keacakan dari sebuah plainteks, bagaimana kita dapat menganalisis teks yang diacak dengan menggunakan algoritma tertentu.

- Analisis Statistika
  Ini merupakan teknik dalam menganalisis kode chiperteks yang muncul dan memasangkannya dengan sebuah plainteks dan chiperteks lain sehingga dapat diektahui pola algoritma enkripsi kriptografi tersebut.

- *Brute Force Search*
  Ini merupakan teknik terakhir, yakni ketika

[1]orang yang melakukan proses enkripsi plainteks

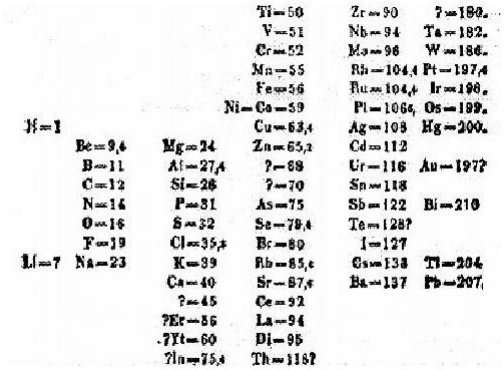
sebuah chiperteks tidak bisa dipecahkan maka dilakukan percobaan pada setiap kemungkinan. Hal ini bisa sangat lama ketika kode yang harus diterjemahkan sangat panjang.

Saat ini, *cryptoanalyst* menjadi sangat populer. Banyak orang yang mulai tertarik dengan pemecahan kriptografi, menjadikan hal ini menjadi sebuah hobi tersendiri. Bahkan, sudah beberapa tahun belakangan ini diadakan Olimpiade Bahasa Internasional (*International Language Olympiad*). ILO merupakan olimpiade yang menjadikan penerjemahan suatu bahasa lokal penduduk di suatu tempat menjadi sebagai soal yang diujikan. Hal ini, sangat sulit sebab hanya sekitar ratusan bahkan puluhan orang saja yang menggunakan bahasa tersebut. Bahasa asing ini, bisa diibaratkan sebagai sebuah chiperteks dan mereka harus menemukan sebuah plainteksnya yang berbentuk bahasa inggris. Dalam menyelesaikan soal tersebut, mereka dituntut untuk menggunakan kriptoanalisis dalam memecahkan soalnya.

1.2 Tabel Periodik

Sekitar tahun 1869 dan 1870 Dmitri Mendelèev dan Lothar Meyer menyatakan bahwa sifat-sifat unsur kimia dapat direpresentasikan sebagai fungsi periodik dari massa atom unsur tersebut dan inilah gagasan munculnya tabel periodik. Tabel periodik merupakan tabel yang berisi daftar unsur-unsur kimia yang disusun berdasarkan kesamaan sifat dari unsur-unsur tersebut[1]. Saat pertama kali muncul tabel periodik disusun berdasarkan kenaikan massa atom, namun setelah diketahui bahwa atom memiliki isotop[2] sehingga penyususunan tabel periodik diubah menjadi kenaikan nomor atom.

Tabel periodik merupakan tabel yang unik, penyusunannya yang berdasarkan sifat periodik unsur menjadikan dia tidak mengalami perubahan ketika ada unsur baru yang ditemukan. Ketika Mendelèev pertama kali mempublikasikannya, ia juga mampu meramalkan unsur yang belum ditemukan beserta sifatnya. Ia meramalkan bahwa akan ada 3 unsur baru yang akan ditemukan 1 mirip Boron (B) dan menamainya Ekaboron (Eb), 1 mirip Silikon (Si) ia menamainya Ekasilikon (Es), dan 1 mirip Alumunium ia menamainya Ekaalumunium. Pada 15 tahun kemudian, 3 unsur tersebut di temukan. Ekaboron dinamai Scandium (Sc), Ekasilikon dinamai Germanium (Ge), dan Ekaalumunium dinamai Galium (Ga)[4].



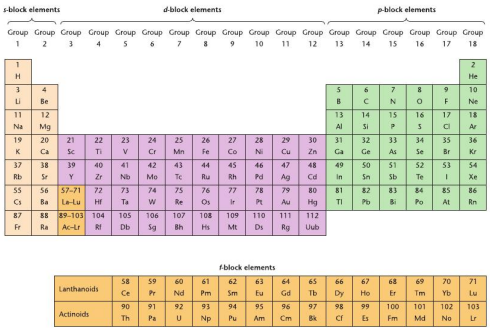
Gambar 2: Tabel Periodik Pada Zaman Mendelèev

Sekarang, tabel periodik terdiri dari 118 unsur, 18 kolom disebut sebagai **golongan**, 7 baris disebut disebut sebagai **periode**, dan 2 baris yang terpisah dari tabel utama yang disebut golongan Aktinida dan Lantanida. Namun, tak semua baris dan kolom tersebut terisi penuh oleh unsur. Baris I hanya berisi 2 unsur yakni di golongan 1 dan 18, untuk baris II dan III hanya terisi 8 unsur golongan 3-12 tidak ada unsur yang menempati tempat tersebut. Baris IV - VII berisi 18 unsur dan pada baris VIII (Lantanida) dan IX (Aktinida) terisi 14 unsur.

Selaim dibagi menjadi 18 golongan unsur dalam tabel periodik juga dibagi beberapa blok. Blok s terdiri dari golongan 1 dan 2, blok p terdiri dari golongan 3 - 18, blok d terdiri dari golongan 3 - 12, blok f terdiri dari golongan lantanida dan aktinida. Golongan tersebut juga memiliki nama masing - masing Golongan 1 disebut sebagai golongan Logam Alkali, golongan 2 disebut sebagai Logam Alkali Tanah, golongan 3 - 12 disebut sebagai Logam Transisi, golongan 15 disebut sebagai golongan Pnictogen, golongan 16 disebut sebagai golongan Kalkogen, golongan 17 disebut sebagai golongan Halogen, golongan 18 disebut sebagai Gas Mulia[3], dan golongan lantanida dan aktinida sebagai Logam Transisi Dalam.

[2]atom dari unsur yang sama namun massa berbeda

[3]disebabkan sukar bereaksi dengan atom lain



Gambar 3: Tabel Periodik Modern

2 Kriptografi Unsur Kimia

Dalam penyandian pesan, umumnya digunakan huruf (kapital dan kecil) serta angka dan karakter. Total karakter yang dipakai hanya sekitar 70 karakter, jika setiap sandi memiliki panjang 6 maka kemungkinan menemukan kode sandi tersebut adalah 70^6 kemungkinan. Untuk sebuah kode yang sangat rahasia, jumlah kemungkinan tersebut masih terlalu kecil sehingga dibutuhkan karakter yang sangat panjang agar sandi tersebut tidak mudah dipecahkan dan keamanan sandi tersebut terjaga.

Tabel periodik yang merupakan sebuah alat yang sangat bermanfa'at dalam ilmu kimia, ternyata dapat menjadi sebuah alat perantara dalam pembuatan chiperteks suatu pesan menggunakan teknik kriptografi. Bentuknya yang 'terkesan' tak beraturan menjadikannya sebagai sebuah penyandi pesan yang baik. Tak disangka ternyata tabel periodik mengandung banyak informasi tentang semua unsur kimia yang telah ditemukan. Semua informasi tersebut dapat digunakan untuk membuat chiperteks dari suatu pesan rahasia dan memvariasikan chiperteks dengan variasi angka, huruf kecil, dan huruf kapital.

Kriptografi menggunakan unsur kimia dalam tabel periodik sebagai penyusun sandi, menjadikan kode yang dihasilkan lebih kompleks sehingga untuk memecahkanya pun menjadi lebih rumit. Unsur yang berada di tabel periodik periodik digunakan sebagai pengganti karakter penyusun sandi sehingga variasi sandi yang dihasilkan bisa jauh lebih banyak, jika sandi memiliki panjang 6 karakter, maka sandi yang dapat dihasilkan 118^6. Jumlah ini 23 kali lebih banyak jika dibandingkan menggunakan karakter biasa. Selain itu, letak unsur dalam tabel periodik yang unik pun dapat dijadikan bagian sebagai proses enkripsi dari plainteks.

Dalam tabel periodik, unsur diletakkan sesuai dengan golongan dan periodenya serta tersusun berdasarkan kenaikan atom. Hal ini menjadikannya sebuah koordinat baru yang dapat direpresentasikan menggunakan sebuah bilangan. Tabel periodik yang juga berisi nomor atom pun dapat dijadikan sebuah bahan penyusunan chiperteks. Ketika kita telah menunjukkan kode suatu atom, maka kita dapat mengambil nilai nomor atom atom kemudian memodifikasikannya menjadi sebuah chiperteks yang hanya berisi sebuah angka tak bermakna. Sifat periodik dari suatu unsur, dikelompokkan dengan penyatuan unsur-unsur tersebut dalam suatu golongan. Dalam hal ini, kita dapat memanfa'atkannya dengan membuat algoritma pertukaran dari unsur-unsur tersebut sehingga menghasilkan sebuah chiperteks yang berisi lambang unsur tertentu.

Pengunaan tabel periodik sebagai sarana pembuatan chiperteks menjadi sangat bermanfa'at dan menghasilkan kode yang unik dan jarang dilihat sehingga kerahasiaan sebuah pesan menjadi lebih terjaga.

2.1 Algoritma Kriptografi Unsur Kimia

Sebagai contoh, kita gunakan chiperteks sebuah lambang unsur.
Algoritma yang digunakan dalam kriptografi unsur kimia sebagai berikut :

1. Pilih sebuah angka 'a' antara 1-19 yang harus dirahasiakan
2. Lakukan proses enkripsi dengan cara mengambil 3 digit angka
   - Angka pertama sebagai baris dari dalam tabel periodik
   - Dua angka setelahnya sebagai kolom dengan cara $c_i = p_i \mod a$
3. Tampilkan lambang unsur yang menunjukkan lokasinya
4. Jika lokasi di tabel periodik tidak mengandung unsur, maka chiperteks ketiga angka tersebut $c_i = p_i \mod a$
5. Jika angka pertama adalah 0, maka chiperteks untuk ketiga angka tersebut $c_i = p_i \mod a$

6. Jika angka kurang dari 3 digit, maka chiperteks untuk ketiga angka tersebut $c_i = p_i \mod a$

7. Proses deskripsi dilakukan dengan cara $p_i = a.k + c_i$; k = 0, 1, 2,...

Sebagai ilustrasi, misalkan pesan plainteks yang akan disandikan P = HARI INI (dengan desimal ASCII-nya 7265827332737873). Pecah P menjadi blok masing-masing berisi maksimal 3 digit angka. Kita ambil a = 10.

$p_1 = 726$ $p_4 = 273$
$p_2 = 582$ $p_5 = 787$
$p_3 = 733$ $p_6 = 003$

maka

$c_1 = Sg$ $c_4 = 3$
$c_2 = Sr$ $c_5 = Bh$
$c_3 = Ac$ $c_6 = 3$

C = SgSrAc3Bh3
Pengembalian chiperteks menjadi plainteks, menggunakan algoritma $p_i = a.k + c_i$.

$c_1 = Sg$ $c_4 = 3$
$c_2 = Sr$ $c_5 = Bh$
$c_3 = Ac$ $c_6 = 3$

- Pertama, lihat letak tiap unsur pada tabel periodik, dan ambil digit pertama yang ditunjukkan oleh baris unsur tersebut.

- Kedua, hitung nilai 2 digit sisanya $p_i = a.k + c_i$

$p_1 = 726$ $p_4 = 273$
$p_2 = 582$ $p_5 = 787$
$p_3 = 733$ $p_6 = 003$

Algoritma yang kita gunakan sangat sederhana, tetapi dapat menghasilkan sandi yang memiliki kombinasi angka, huruf kapital dan huruf kecil jika kita dapat memodifikasi algoritma yang digunakan, maka chiperteks menjadi sulit untuk dipecahkan, ditambah lagi jika kita tidak hanya menggunakan lambang unsur sebagai chiperteks tetapi juga menggunakan sifat unsur yang dideskripsikan di tabel periodik.

3 Keunggulan Kriptografi Unsur Kimia

3.1 Objek yang digunakan luas dan dapat berkembang

Kriptografi menggunakan metode ini menjadikan objek yang dipakai lebih luas tidak hanya angka dan huruf, sehingga menghasilkan banyak kemungkinan dalam memecahkan chiperteks. Selain itu, tabel periodik dapat terus berkembang seiring dengan ditemukannya unsur sintetis sehingga penyandian menjadi semakin luas.

3.2 Algoritma dapat dikembangkan

Dalam tabel periodik tidak hanya terkandung lambang unsur, tetapi juga menggambarkan sifat fisik dan kimia dari unsur tersebut sehingga chiperteks yang dihasilkan tidak hanya berupa lambang unsur tetapi juga senyawa yang dihasilkan maupun sebuah angka yang dapat mencirikan unsur tersebut.

Bentuk tabel periodik yang terdiri dari baris dan kolom pun dapat dimodifikasikan sehingga kita tidak hanya dapat mengambil lambang unsur sebagai chiperteks tetapi juga kombinasi angka dari baris dan kolom tersebut. Ditambah lagi, sifat periodik dari unsur-unsur tersebut juga dapat dipakai sebagai salah satu bentuk algoritma yang dapat menyandikan sebuah pesan rahasia. Maka, ketika sebuah unsur ditemukan, maka algoritma ini akan memiliki 3 buah tempat baru untuk dijadikan kombinasi chiperteks, yakni pada lambang unsur, baris dan kolom unsur, sifat periodik unsur tersebut terhadap unsur lain.

3.3 Kekuatan Algoritma

Jika sandi ini dipecahkan secara manual, dari baris kode pertama telah diketahui maka 2 bilangan digit setelahnya ada 100 kemungkinan jika ada 8 digit bilangan maka ada 10^{16} kemungkinan. Jika suatu komputer mampu memproses 1 juta kemungkinan dalam 1 detik maka butuh 317 tahun dalam menyelesaikannya. Perhitungan ini dilakukan dengan hanya melibatkan lambang unsur didalamnya jika kita memodifikasikannya dengan sifat periodiknya maka akan lebih banyak lagi kode yang dapat tercipta.

4 Kelemahan Kriptografi Unsur Kimia

4.1 Banyak Kasus Khusus

Bentuk tabel periodik yang memiliki kekosongan unsur di banyak tempat menjadikan algoritma ini kurang universal untuk digunakan sehingga banyak kondisi yang harus di buat analisis kasusnya. Banyaknya kasus khusus yang ditangani menjadikan algoritma ini belum sempurna dalam segi keteratutan penyandian sehingga ketika proses deskripsi dilakukan akan muncul beberapa plainteks dan penerima pesan harus memilih mengenai plainteks yang paling tepat.

4.2 Tabel Periodik Bukan Hal Umum

Tidak semua penerima pesan plainteks memahami penggunaan tabel periodik sehingga meskipun telah mengetahui kata sandi, penerima belum tentu bisa memecahkannya. Penggunaan sandi ini hanya dibatasi oleh orang yang dapat mengerti penggunaan tabel periodik.

5 Kesimpulan

Kriptografi Unsur Kimia merupakan salah satu variasi dalam mengembangkan kriptografi. Kriptografi jenis ini, belum pernah ada sebelumnya. Hal ini merupakan sebuah terobosan baru dalam mengembangkan kriptografi. Kriptografi unsur kimia harus terus dikembangkan agar algoritmanya menjadi lebih kompleks dan dapat menjadi algoritma alternatif yang digunakan sebagai proses kriptografi sebuah sandi rahasia.

Kriptografi ini menggunakan informasi yang ada di tabel periodik sebagai sebuah referensi untuk membuat chiperteks dari suatu plainteks. Hal ini menjadikan tabel periodik dapat bermanfaat tidak hanya sebagai penyimpan informasi unsur tetapi juga menjadi sebuah alat penyandi baru yang dapat dikembangkan lebih luas. Kriptografi ini menunjukkan sebuah pemanfaatan lain tabel periodik di bidang Informatika dalam kasus pembuatan kriptografi.

6 *Acknowledgement*

Terima kasih kepada Allah *Subahanallahu wa Ta'ala* atas rahmat dan karunia-Nya sehingga saya dapat menyelesaikan makalah saya yang berjudul *Kriptografi Unsur Kimia dalam Tabel Periodik*, serta kepada dosen pengajar IF2091 yang telah memberikan bimbingannya selama ini sehingga makalah ini dapat selesai dengan sebaik-baiknya. Dan juga kepada orang tua yang telah memberikan kasih sayang, uang serta waktunya untuk mendidik saya serta teman-teman yang selalu mendukung saya dalam pembuatan makalah ini sehingga makalah ini dapat selesai tepat waktu.

Daftar Gambar

Pustaka

[1] Housecrouft, Catherine E. Sharpe, Alan G. *Inorganic Chemistry* 2^{nd} *edition*. Edinburg : Pearson Prentice Hall, 2005.

[2] Kromodimoeljo, Sentot. *Teori dan Aplikasi Kriptografi*. Jakarta : SPK IT Consulting, 2010

[3] Munir, Rinaldi. *Matematika Distrit*. Bandung: Informatika, 2005.

[4] *Preparatory Problems* 39^{th} *International Chemistry Olympiad*

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, 19 Desember 2012

Lukman Hakim (13511004)