Analisis Pemanfaatan Algoritma Kriptografi *One-Time Pad* Berbasis DNA untuk Menghasilkan Cipher yang Tidak Dapat Dipecahkan (*Unbreakable Cipher*)

David Susanto [1)]

1) Jurusan Teknik Informatika ITB, Bandung 40132, email: if14019@students.if.itb.ac.id

Abstraksi *– Algoritma kriptografi One-Time Pad (OTP) merupakan satu-satunya algoritma kriptografi sempurna yang mampu menghasilkan cipherteks yang tidak dapat dipecahkan (unbreakable cipher) hingga saat ini. Akan tetapi, masalah kepraktisan dalam penerapan algoritma ini menyebabkan OTP tidak dipergunakan secara universal. Panjang kunci yang harus sama dengan panjang plainteks menyebabkan algoritma ini mengalami masalah dalam penyimpanan dan pendistribusian kunci saat dipergunaan untuk mengenkripsi pesan yang panjang. Selain itu pembangkitan kunci secara acak tidak dapat dilakukan secara simultan sehingga pengirim pesan harus mengirimkan kunci terlebih dahulu kepada penerima pesan. Hal ini membawa masalah baru dalam keamanan dan biaya yang diperlukan selama proses pengiriman kunci tersebut.*

Hasil penelitian terbaru menemukan kemampuan DNA (deoxyribonucleic acid) sebagai media komputasi dan penyimpanan yang sangat padat (ultra-compact). Hasil penilitan ini membuka peluang bagi DNA untuk dimanfaatkan sebagai media penyimpanan pada algoritma kriptografi OTP. Pada makalah ini akan dijabarkan bagaimana penerapan OTP berbasis DNA dengan melakukan metode substitusi dan skema XOR memanfaatkan kunci acak.

Di dalam makalah ini akan dijabarkan pula analisis pemanfaatan OTP berbasis DNA tersebut untuk menghasilkan unbreakable cipher ditinjau dari segi keamanan dan kekuatannya terhadap serangan, kepraktisan dalam penerapannya sebagai salah satu cara pengamanan informasi yang dapat dipergunakan secara universal.

.

Kata Kunci*: One-Time Pad, kriptografi berbasis DNA, unbreakable cipher, metode substitusi, skema XOR, DNA chip.*

1. PENDAHULUAN

Hingga saat ini telah banyak usaha yang dilakukan para ahli kriptografi untuk menciptakan algoritma kriptografi yang mampu menghasilkan pesan cipher yang tidak dapat dipecahkan (*unbreakable cipher*). Namun hingga saat tulisan ini dibuat, hanya ada satu algoritma kriptografi yang mampu menghasilkan unbreakable cipher, yaitu algoritma One-Time Pad (OTP). Algoritma OTP yang ditemukan oleh Major Joseph Mauborgne pada tahun 1917, memanfaatkan kunci yang sifatnya acak dengan panjang yang sama dengan panjang plainteks yang dienkripsikan sebagai syarat untuk menghasilkan *unbreakable cipher*.

Walaupun algoritma ini mampu menghasilkan *unbreakable cipher*, namun pemanfaatannya masih sangat jarang karena masalah kepraktisan. Panjang kunci yang harus sama dengan panjang plainteks menyebabkan algoritma ini mengalami masalah dalam penyimpanan dan pendistribusian kunci saat dipergunaan untuk mengenkripsi pesan yang panjang. Selain itu pembangkitan kunci secara acak tidak dapat dilakukan secara simultan sehingga pengirim pesan harus mengirimkan kunci terlebih dahulu kepada penerima pesan. Hal ini membawa masalah baru dalam keamanan dan biaya yang diperlukan selama proses pengiriman kunci tersebut.

DNA (*deoxyribonucleic acid*) makhluk hidup memiliki kemampuan yang sangat besar sebagai media penyimpanan informasi. Kompleksitas susunan rangkaian pita protein yang dimiliki DNA menyebabkannya memiliki kemampuan yang tinggi dalam menghasilkan kombinasi kode-kode sehingga mampu menjadi media penyimpanan yang sangat padat (*ultra-compact*). DNA, bahkan diperkirakan akan menjadi media penyimpanan masa depan menggantikan media penyimpanan konvensional saat ini yang masih berbasiskan bilangan biner (*binary*).

Pengaplikasian OTP yang terbentur oleh keterbatasan ukuran media penyimpanan elektronik konvensional saat ini, dapat dipecahkan dengan memanfaatkan DNA sebagai media penyimpanannya. Sifat DNA yang padat (*compact*) menjadikannya sebagi media yang memadai untuk memenuhi kebutuhan ruang informasi yang besar pada OTP. Hal inilah yang mendasari beberapa ahli kriptografi untuk mengajukan pengkombinasian antara kriptografi berbasis DNA dan algoritma OTP untuk menghasilkan sebuah metode kriptografi baru yang mampu menghasilkan *unbreakable cipher*.

2. TEORI DASAR

2.1. Komputasi Biomolekuler

Komputasi biomolekuler merupakan salah satu upaya pemanfaatan metode bioteknologi untuk melakukan komputasi. Salah satu penerapan komputasi biomolekuler ini adalah pemanfaatan DNA sebagai media untuk komputasi skala ultra (*ultra-scale computation*).

DNA memiliki kemampuan sebagai media penyimpanan informasi yang sangat padat (*ultra-compact*). Kemampuan penyimpanan DNA bahkan sangat jauh melebihi kemampuan media penyimpanan konvensional saat ini seperti memori *flash*, pita magnetik, dan cakram optik. Satu gram DNA mengandung 10^{21} basis DNA. Jika dikonversikan ke dalam satuan *byte*, maka jumlah tersebut setara dengan 10^{8} *tera-bytes*. Dengan kapasitas demikian, dengan beberapa gram DNA saja, kita telah dapat menyimpan seluruh data yang ada dunia.

Agar kemampuan DNA tersebut dapat dimanfaatkan untuk menyimpan informasi dari sistem biner yang pergunakan hingga saat ini, diperlukan konversi dari media penyimpanan konvensional yang berbasis biner ke media penyimpanan berbasiskan DNA, demikian pula sebaliknya. DNA chip arrays dipergunakan sebagai jembatan input dan output data dari DNA ke media penyimpanan konvensional yang berbasis biner. Data biner dapat di encode ke dalam rantai DNA dengan memanfaatkan rentetan alphabet oligonukleotid.

2.2. Kriptografi Berbasis DNA

Keamanan data merupakan masalah yang sangat krusial di era infomasi saat ini. Salah satu cara yang dipergunakan untuk pengamanan data tersebut adalah dengan memanfaatkan kriptografi. Kriptografi yang telah lama dikenal oleh manusia sejak zaman Mesir 4000 tahun yang lalu hingga saat ini.

Pada bidang teknologi informasi, kriptografi dipergunakan sangat luas dalam masalah keamanan data. Telah banyak algoritma kriptografi yang bermunculan. Di antara algoritma-algoritma yang telah ada tersebut memiliki kelebihan dan kekurangan masing-masing.

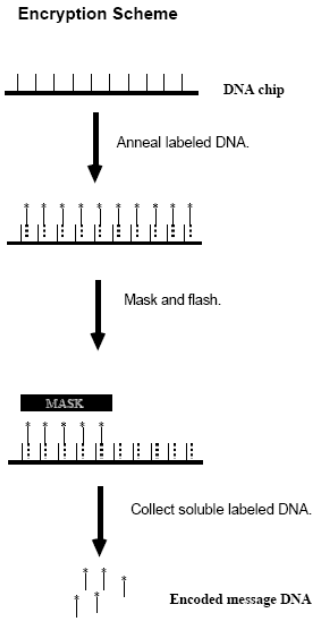
One-Time Pad sebagai salah satu algoritma kriptografi diklaim sebagai algoritma yang mampu menghasilkan cipherteks yang tidak dapat dipecahkan (*unbreakable cipher*). Namun OTP memiliki keterbatasan yang menyebabkan algoritma ini tidak dipergunakan secara universal. Panjang kunci yang harus sama dengan panjang pesan menjadikan algoritma ini susah untuk diimplementasikan karena keterbatasan media penyimpanan apabila menggunakan media penyimpanan konvensional yang ada saat ini.

Perkembangan ilmu pengetahuan terutama di bidang bioteknologi telah memungkinkan DNA sebagai media penyimpanan masa depan dengan kempuan untuk menampung data dengan sangat padat (*ultra-compact*). Hal ini memberikan peluang bagi DNA untuk medukung bidang kriptografi dalam masalah media penyimpanan. Aplikasi DNA dalam bidang kriptografi yang telah dipergunakan adalah melakukan enkripsi terhadap kode DNA natural dan DNA *encoding binary* data.

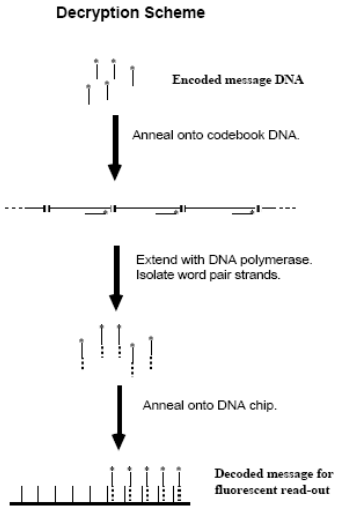
Salah satu skema kriptografi berbasis DNA adalah menggunakan *chip-based micro-array technology* yang juga dikenal dengan istilah DNA *chips*. Skema DNA chips ini akan dikombinasikan pada OTP berbasis DNA untuk melakukan enkripsi dan dekripsi terhadap pesan.

Proses enkripsi dengan menggunakan DNA chips ini dilakukan dengan mengambil input berupa rantai DNA yang kita anggap sebagai pesan plainteks. Kemudian input ini ditempelkan pada rantai *key* tertentu untuk menghasilkan tagged plaintext. Tagged plaintext ini kemudian disembunyikan dengan mencampur banyak rantai DNA pengacak lain.

Proses dekripsi DNA chips dilakukan dengan menggunakan rantai kunci. Rantai DNA yang terdekripsi diperoleh dengan melakukan sejumlah metode separasi DNA rekombinan. Metode tersebut dilakukan dengan melakukan pemisahan hibridisasi terhadap komplemen rantai kunci yang disiapkan pada permukaan khusus. Langkah separasi ini dapat dikombinasikan dengan langkah amplifikasi. Prosedur tersebut diilustrasikan dengan gambar berikut.



Gambar 1: Prosedur enkripsi berbasis DNA

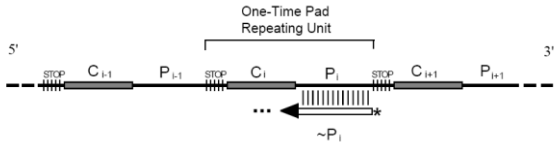


Gambar 2: Prosedur dekripsi berbasis DNA

3. IMPLEMENTASI

3.1. OTP berbasis DNA dengan metode subsitusi

Implementasi algoritma One-Time Pad berbasis DNA dengan metode substitusi dilakukan dengan memetakan sebuah plainteks menjadi cipherteks dengna menggunakan sebuah DNA pad yang panjang. DNA pad tersebut mengandung banyak segmen. Setiap segmen mengandung sebuah kata cipher (*cipher word*) diikuti oleh sebuah kata plainteks (*plaintext word*). Setiap *cipher word* ditempelkan dengan sebuah *plaintext word* untuk menciptakan pasangan kata (*word-pair*). Rantai DNA pasangan kata ini akan dipergunakan sebagai *lookup table (pad)* dalam pemetaan plainteks menjadi cipherteks.



Gambar 3: One-Time Pad berbasis DNA

Setiap unit segmen yang pada *pad* DNA terdiri dari:

- B_i, merupakan *cipher word* dengan panjang $L_1 = c_1 \log n$
- C_i, merupakan *plaintext word* dengan panjang $L_2 = c_2 \log n$
- Untuk memisahkan setiap pasangan *cipher word* dan *plaintext word* dengan pasangan berikutnya, diberikan sebuah "*stopper*" yang memiliki panjang $L_3 = c_3$

Misalnya panjang rantai DNA adalah *n*, maka jumlah segmen yang dimiliki sebuah *pad* adalah:

$$d = n/(L_1+L_2+L_3)$$

Proses enkripsi pada metode substitusi ini dilakukan dengan cara melakukan substitusi setiap DNA *plaintext word* dengan DNA *cipher word* padanannya. Proses ini dilakukan pada setiap segmen yang ada hingga akhir pad DNA.

3.2. OTP berbasis DNA dengan skema XOR

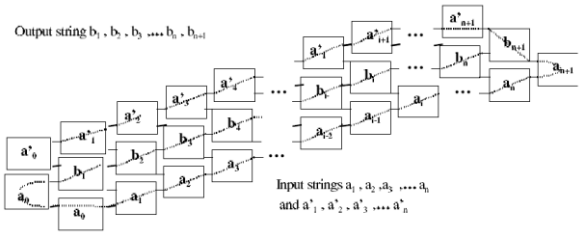
Pada algoritma One-Time Pad berbasis DNA dengan skema XOR, implementasi dilakukan dengan memanfaatkan prinsip *Vernam cipher*. *Vernam cipher* memanfaatkan fungsi XOR untuk menghasilkan cipherteks. Misalnya P adalah bit plainteks, kemudian P akan dienkripsi menjadi cipherteks C dengan menggunakan kunci *k*, maka cukup melakukan operasi XOR antara P dan *k* untuk menghasilkan C.

$$C = P \text{ XOR } k$$

Sementara untuk melakukan dekripsi,Vernam cipher memanfaatkan sifat komutatif dari XOR.

$$\begin{aligned} C \text{ XOR } k &= (P \text{ XOR } k) \text{ XOR } k \\ &= P \text{ XOR } (k \text{ XOR } k) \\ &= P \end{aligned}$$

Masing-masing plainteks harus ditempelkan pada *prefix index tag* yang unik dengan panjang L_0 untuk menghasilkan indeks bagi plainteks tersebut. Setelah itu masing-masing deretan OTP DNA harus ditempelkan pada *prefix index tag* unik dengan panjang yang sama yaitu L_0 untuk menghasilkan komplemen dari plainteks.



Gambar 4: Komputasi XOR menggunakan DNA

Untuk melakukan cipher dilakukan operasi bit XOR dengan cara tiap fragmen dari plainteks dioperasikan terhadap *pad* DNA. Dengan menggunakan teknik rekombinan DNA kemudian dilakukan konkatenasi setiap pasang plainteks dan *pad* menjadi sebuah rantai DNA.

4. ANALISIS

4.1. Analisis Kekutatan OTP berbasis DNA

OTP dengan memanfaatkan DNA ini pada dasarnya memiliki kekuatan yang sama dengan kekuatan yang dimiliki oleh OTP biasa. Pada OTP biasa cipherteks yang dihasilkan tidak dapat dipecahkan karena memiliki sifat memiliki kunci yang acak dan panjang kunci harus sama dengan panjang plainteks.

Karena kemampuan DNA untuk menampung data secara padat, maka panjang kunci yang sama panjangnya dengan panjang plainteks dimungkinkan. Hal ini menyebabkan kekuatan OTP dalam menghasilkan cipher yang tidak dapat dipecahkan dapat kita pergunakan dengan maksimal.

Selain itu keragaman pad yang dimiliki juga mendukung OTP untuk menghasilkan cipher teks yang tidak dapat dipecahkan. Dalam menghasilkan sebuah pad keragaman yang dapat dihasilkan dapat diperoleh bergantung pada kondisi:

1. Ukuran kamus yang dipergunakan.
2. Jumlah kemungkinan pad yang tersedia.
3. Ukuran, kompleksitas, dan frekuensi transmisi data.

Untuk itu kita pergunakan parameter yang sesuai dengan yang ada di atas.

Tabel 1. Parameter analisi keragam pad

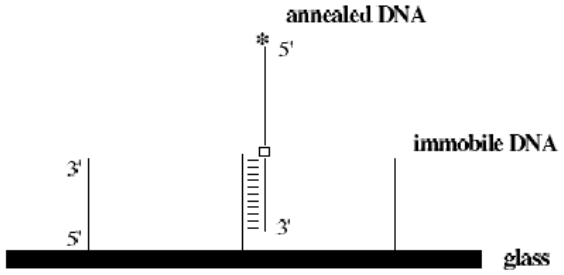
Parameter	Nilai
Ukuran kamus	10.000-250.000 kata
Ukuran kata	8-24 huruf
Ukuran pesan	5-30% dari ukuran kamus
Kemungkinan *pad*	10^6-10^8

Misalnya dipergunakan contoh nukleotid N = A+C+G+T, R = A+G, Y = C+T. Kemudian terdapat rantai dengan deretan RNNYRNRRYN. Dengan menggunakan parameter dihasilkan kamus dengan kemungkinan sebanyak: 2x4x4x2x2x4x2x2x2x4 = 16.384 kemungkinan.

4.2. Analisis Kepraktisan OTP berbasis DNA

Dengan menggunakan DNA sebagai basis untuk menyimpan pesan, penerapannya pada OTP menjadi sangat praktis. Berikut beberapa hal yang menjadikan OTP berbasis dapat praktis dipergunakan:

1. Kemudahan dalam melakukan enkripsi informasi oleh pengirim. Pengirim pesan tidak membutuhkan banyak informasi untuk melakukan *encoding*.
2. Informasi yang harus dilewatkan pada jalur komunikasi sedikit, karena cukup kunci saja. Ukuran kunci ini proporsional terhadap ukuran plainteks dengan rasio yang kecil.
3. Informasi dalam bentuk protein pada DNA dapat ditransferkan melalui public channel dan ukuran informasi yang disimpan dalam bentuk protein umumnya lebih kecil daripada ukuran informasi aslinya.



Gambar 5: Komponen dan organisasi DNA chip

Namun dibalik kelebihan yang ditawarkan tersebut, penggunaan DNA sebagai media penyimpanan masih jarang dipergunakan karena peralatan komputasi seperti prosesor yang berbasis DNA masih belum tersedia di pasar sehingga diperlukan media perantara seperti DNA *chips* yang mungkin tidak lazim di temukan. Apabila sistem komputer tidak lagi menggunakan sistem biner, maka DNA merupakan alternatif yang sangat mungkin untuk menggantikan sistem komputer yang ada saat ini.

5. KESIMPULAN

Penggunaan DNA untuk mendukung algoritma kriptografi One-Time Pad telah dapat memecahkan kesulitan yang dialami selama ini dalam masalah media penyimpanan. Hal ini menjadikan OTP berbasiskan DNA merupakan algoritma kriptografi yang sempurna yang dapat menghasilkan *unbreakable cipher*. Tetapi OTP berbasis DNA belum siap untuk dipergunakan dalam kehidupan sehari-hari karena sistem komputasi yang berbasis DNA masih sangat jarang dipergunakan.

DAFTAR REFERENSI

[1] Munir, Rinaldi. "*Diktat Kuliah IF5054 Kriptografi"*. Institut Teknologi Bandung, 2006.

[2] Kang, Nin. "A Pseudo DNA Cryptography Method". National University of Singapore, 2004.

[3] Gehani, Ashish; Thomas LaBean dan John Reif. "*DNA-based Cryptography"*. Duke University, 1999