Modifikasi *Vigenere Cipher* dengan Enkripsi-Pembangkit Kunci Bergeser

Anggrahita Bayu Sasmita, 13507021

Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung
e-mail: if17021@students.if.itb.ac.id; angga.sasmita@gmail.com

Abstrak

Makalah ini membahas sebuah modifikasi dari suatu algoritma enkripsi klasik Vigenere Cipher. Modifikasi tersebut dilakukan dengan penambahan suatu tahapan "enkripsi" yang menghasilkan suatu kunci kembangan sehingga panjang kunci tersebut sama dengan panjang plainteks yang disediakan untuk dienkripsi pada cipher ini.

*Penulis memberi nama modul dan metode pengaya kunci tersebut sebagai Enkripsi-Pembangkit Kunci Bergeser (*Shifting Key Generator-Encryption*). Pembangkit kunci ini akan melakukan suatu metode tertentu untuk menambahkan kunci yang diberikan pengguna sehingga kunci tersebut menjadi sama panjang dengan plainteks.*

Metode enkripsi Vigenere Cipher dikenal sebagai metode yang aman dalam melakukan enkripsi suatu dokumen hingga dirancangnya beberapa metode pemecahan kunci seperti metode Kasiski atau metode Friedman yang diperkuat dengan analisis numerik berdasarkan frekuensi kemunculan susunan huruf majemuk pada cipherteks yang dihasilkan dari enkripsi. Metode enkripsi Vigenere Cipher dinilai tidak aman lagi setelah dirancangnya metode-metode tersebut.

Salah satu algoritma enkripsi yang hingga saat ini tidak dapat memungkinkannya cipherteks dipecahkan adalah dengan metode/prinsip one-time pad atau suatu metode yang dikenal sebagai Vernam Cipher. Kesamapanjangan kunci-dengan plainteks merupakan satu penerapan dari prinsip metode enkripsi tersebut. Dengan kunci yang sama panjang dengan plainteks, enkripsi melalui metode ini dapat menghasilkan suatu cipherteks yang memiliki pengulangan minimum dan hampir tidak dapat dicari kuncinya melalui analisis frekuensi.

Kata kunci: *kriptografi, vigenere cipher, vernam cipher, pembangkit kunci bergeser*

1. PENDAHULUAN

1.1 Latar Belakang

Algoritma enkripsi *Vigenere Cipher* merupakan suatu teknik kriptografi klasik yang tergolong sebagai metode substitusi abjad majemuk. Dalam pengimplementasiannya, algoritma ini dapat dianggap tidak aman setelah disusunnya Metode Kasiski yang dapat memecahkan cipherteks yang telah dienkripsi melalui algoritma tersebut. Metode Kasiski memanfaatkan pola pengulangan yang terjadi di dalam cipherteks untuk menemukan kunci yang cocok sehingga pada akhirnya plainteks dapat ditemukan menggunakan kunci tersebut. Secara tidak langsung, metode pemecahan tersebut mengeksploitasi kecenderungan panjang kunci yang relatif lebih pendek daripada panjang plainteks.

Hingga pada saat ini, salah satu metode kriptografi klasik yang tidak dapat dipecahkan adalah metode *one-time-pad*. Metode ini menerapkan sejumlah kunci dengan panjang yang sama dengan plainteks untuk menyusun cipherteks dengan substitusi yang serupa dengan metode *Vigenere Cipher*.

Berdasarkan kedua persoalan di atas, penulis merumuskan suatu modifikasi terhadap metode *Vigenere Cipher* dengan melakukan pembangkitan kunci sehingga panjangnya sama dengan plainteks sekaligus melakukan enkripsi ganda dengan pencerminan kunci tersebut. Pembangkitan kunci yang dilakukan adalah dengan cara menggandakan kunci, menggeser pola kunci yang telah digandakan, dan melakukan "enkripsi" terhadap kunci awal dengan metode *Vigenere*. Kunci yang "terenkripsi" tersebut dikonkatenasi terhadap kunci awal hingga panjang kunci sama dengan panjang plainteks. Setelah kunci tersebut terbentuk, maka substitusi dilakukan terhadap plainteks sehingga membentuk cipherteks.

Modifikasi ini diberlakukan untuk menghasilkan cipherteks yang bebas dari pengulangan pola yang memungkinkannya tereksploitasi oleh pemecahan metode kasiski. Dengan metode ini, penulis berhipotesis bahwa cipherteks yang dihasilkan memiliki kerahasiaan sebagaimana cipherteks yang dihasilkan metode kriptografi *one time pad*, namun dengan sumber daya yang relatif lebih ringan.

1.2 Tujuan

Tujuan penulisan makalah mengenai modifikasi *Vigenere Cipher* ini adalah untuk melakukan pembelajaran pada bidang kriptografi sekaligus merancang suatu metode *cipher* klasik yang aman dengan basis *Vigenere Cipher*.

1.3 Rumusan Masalah

Pada pembahasan makalah ini, penulis merumuskan beberapa masalah, antara lain:

1. Bagaimana menghasilkan kunci secara sistematis sehingga mampu menghasilkan panjang kunci internal yang sama dengan panjang plainteks?
2. Bagaimana cipherteks yang dihasilkan dari substitusi plainteks terhadap kunci tidak mungkin dipecahkan melalui analisis frekuensi?

1.4 Batasan Masalah

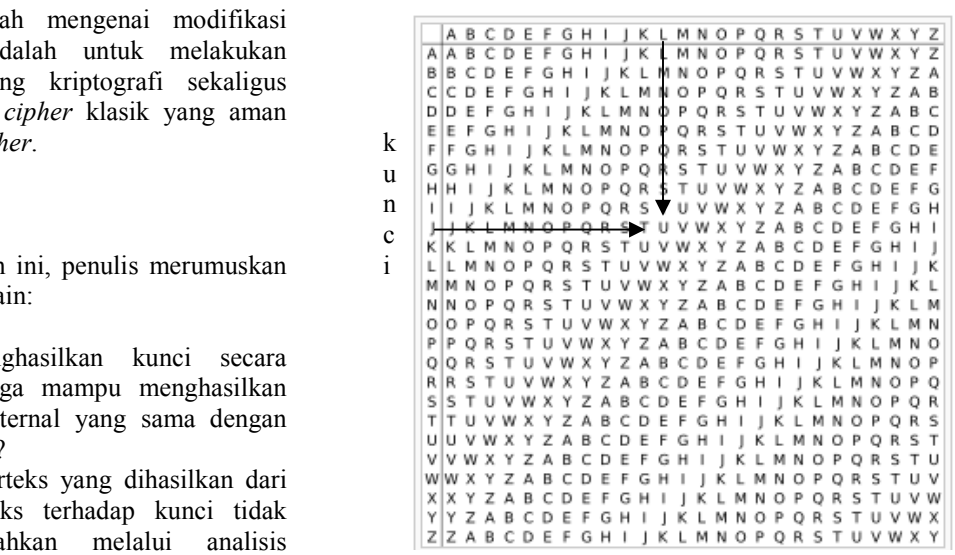
Pada makalah ini, penulis membatasi permasalahan terhadap aspek teknis dalam modifikasi *Vigenere Cipher* sebagaimana telah dibahas dalam rumusan masalah dan latar belakang. Adapun aspek-aspek seperti kompleksitas algoritma atau implementasi dalam bahasa pemrograman tertentu adalah di luar pembahasan makalah ini.

2. DASAR TEORI

2.1 *Vigenere Cipher* dan metode kriptanalisis sederhana

Salah satu metode enkripisi adalah menggunakan metode enkripsi abjad majemuk manual. Representasi enkripsi abjad majemuk manual tersebut salah satunya adalah metode *Vigenere Cipher*. Metode ini dirancang pada abad XVI oleh seorang diplomat merangkap kriptolog dari Prancis bernama Blaise de Vigenere. Metode enkripsi ini mulai dipublikasi pada tahun 1856, dua abad setelah algoritma ini dirancang. Metode enkripsi ini sempat digunakan dalam pengiriman pesan ketika Perang Saudara Amerika oleh Tentara Konfederasi. Akibat dekripsi pesan inilah peperangan pada saat itu terjadi.

Dalam implementasinya, *Vigenere Cipher* memanfaatkan pemetaan melalui Persegi Vigenere. Persegi ini menyimpan sederetan huruf-huruf tersusun yang merupakan pemetaan antara karakter kunci (baris) terhadap karakter plainteks (kolom) yang menghasilkan titik temu pada cipherteks (sel).



Gambar 1 Persegi Vigenere dan contoh metode pembentukan cipherteksnya (plainteks "L" dengan kunci "J" menghasilkan cipherteks "U")

Pemetaan *Vigenere Cipher* melalui Persegi Vigenere tersebut dapat direpresentasikan melalui suatu penjumlahan bilangan bulat yang diperkaya dengan operasi aritmetika modulo. Karakter pada plainteks maupun kunci diwakilkan sebagai bilangan bulat dari 0 hingga 25 sesuai urutan alfabetik. Representasi bilangan bulat tersebut kemudian dijumlahkan dan di-modulo dengan bilangan 26. Bilangan 26 ini merupakan jumlah total karakter alfabet yang umum digunakan. Pengoperasian tersebut akan menghasilkan suatu bilangan bulat antara 0 hingga 25 yang relatif berbeda (mungkin sama) dengan representasi bilangan bulat karakter plainteks. Bilangan hasil inilah yang akan digunakan untuk memetakan karakter cipherteks.

Proses dekripsi *Vigenere Cipher* serupa dengan enkripsinya. Perbedaannya terdapat pada operasi terhadap representasi bilangan cipherteks yang diubah melalui pengurangan terhadap bilangan representasi kunci. Bilangan bulat hasil pengurangan tersebut kemudian di-modulo dengan bilangan 26

untuk menghasilkan representasi bilangan karakter plainteks.
Secara matematis, proses enkripsi *Vigenere Cipher* dapat dirumuskan sebagai berikut:

$$C_i = (P_i + K_i) \bmod 26$$

sedangkan proses dekripsinya:

$$P_i = (C_i - K_i) \bmod 26$$

dalam hal ini,

P_i: karakter plainteks;
C_i: karakter cipherteks;
K_i: karakter kunci.

Suatu keunggulan yang ditawarkan melalui enkripsi *Vigenere Cipher* adalah kemampuan cipherteks untuk tidak dapat dipecahkan melalui analisis frekuensi sederhana maupun analisis kontak yang mendukungnya.

Analisis frekuensi memanfaatkan banyaknya kemunculan suatu karakter pada suatu kalimat dalam bahasa tertentu. Hal tersebut menyebabkan cipher abjad tunggal dapat dengan mudah dipecahkan karena untuk suatu bahasa, terdapat statistik yang menunjukkan persentase suatu karakter muncul dalam kalimat dalam bahasa tertentu. Kriptanalis hanya perlu mencocokkan huruf yang sering muncul pada cipherteks dengan karakter yang bersesuaian pada statistik.

Analisis frekuensi diperkuat melalui analisis kontak. Dengan dukungan analisis kontak, maka dilakukan pula penghitungan suatu pola rangkaian karakter yang sering muncul dalam suatu bahasa. Pola karakter tersebut dapat berupa bigram (rangkaian dua karakter), trigram (rangkaian tiga karakter), quartogram (rangkaian empat karakter), dan seterusnya.

Sebagai contoh atas analisis frekuensi, misalnya terdapat sebuah cipherteks yang diketahui berisi pesan terenkripsi dalam bahasa inggris. Melalui analisis frekuensi, dapat diketahui jumlah kemunculan karakter pada cipherteks tersebut. Karakter-karakter yang dihitung jumlah kemunculannya tersebut kemudian dibandingkan dengan statistik yang menunjukkan informasi mengenai karakter dan frekuensi kemunculannya dalam bahasa inggris. Sebagaimana informasi, diketahui bahwa karakter-karakter yang berfrekuensi kemunculan tinggi dalam bahasa inggris adalah karakter e, t, a, o, i, dan n. Karakter-karakter berikutnya umumnya tidak memiliki distribusi tetap. Karakter-karakter hasil analisis frekuensi cipherteks kemudian dicocokkan dengan karakter tersebut untuk di-substitusi. Sebagai penguat, analisis kontak diberlakukan terhadap cipherteks untuk mencari pola rangkaian yang berfrekuensi tinggi pada teks. Rangkaian tersebut kemudian disesuaikan dengan rangkaian karakter dalam bahasa inggris yang memiliki kemunculan tinggi, misalnya rangkaian karakter “the”, “and”, “not” dan sebagainya.

Sifat dari enkripsi menggunakan metode *Vigenere Cipher* memberlakukan substitusi yang tidak tentu untuk sebuah karakter. Oleh karenanya, dalam beberapa masa, metode enkripsi ini dianggap sebagai metode yang aman karena tidak dapat dipecahkan menggunakan analisis frekuensi sederhana.

Salah satu atribut lain yang dimiliki metode enkripsi *Vigenere Cipher* ini adalah penggunaan kunci yang dikonkatenasi secara berulang apabila panjang kunci kurang dari panjang plainteks. Konkatenasi kunci ini dilakukan dengan menambahkan karakter yang sama dengan urutan karakter pada kunci hingga jumlah karakter kunci yang diperkaya sama dengan panjang plainteks. Konkatenasi ini merupakan titik lemah dari enkripsi *Vigenere Cipher* yang dapat dieksploitasi untuk melakukan pemecahan terhadap cipherteks hasil enkripsinya.

2.2 Metode Kasiski

Pada pertengahan abad ke-19, suatu metode pemecahan cipherteks *Vigenere Cipher* dirancang oleh seseorang yang digelari ilmuwan komputer oleh kalangan praktisi ilmu komputer saat ini. Dia adalah Charles Babbage. Sebagaimana umumnya sebuah cipher, seorang jurnalis mempublikasikan sebuah cipherteks pada sebuah media cetak dan menantang siapapun untuk memecahkan cipherteks tersebut. Charles Babbage kemudian mengklaim bahwa ia mampu melakukan pemecahan terhadap teks tersebut. Akan tetapi, pada saat itu *Vigenere Cipher* secara umum digunakan pada instansi militer dan pemerintahan sehingga Babbage dihimbau agar mengurungkan publikasi rancangan pemecahannya ke umum.

Publikasi pemecahan *Vigenere Cipher* akhirnya dilakukan oleh seorang matematikawan dari Polandia bernama Friedrich Kasiski pada tahun 1863. Metode ini kemudian teridentifikasi sebagai metode yang serupa dengan proses pemecahan cipherteks yang dilakukan Babbage sebelumnya. Metode ini mengeksploitasi penggunaan kunci yang berulang

pada proses enkripsi. Secara detil, metode tersebut dioperasikan sebagai berikut:

1. Analisis diberlakukan terhadap cipherteks untuk mencari pola-pola karakter berulang. Karakter-karakter dapat diambil minimal tiga rangkaian karakter. Analisis tersebut memberikan hasil berupa jarak-jarak antarpola karakter yang berulang tersebut.

2. Jarak-jarak antarpola karakter yang didapat kemudian dikumpulkan dan dicari nilai pembagi besar bersama-nya. Nilai tersebut diidentifikasi sebagai panjang kunci.

3. Karakter-karakter pada cipherteks kemudian dikelompokkan menjadi *x* kelompok dengan *x* adalah nilai pembagi besar bersama (panjang kunci) yang didapat dari analisis sebelumnya. Karakter dikelompokkan terhadap urutan kemunculannya sebagai karakter ke-1 hingga ke-*x* secara berulang hingga seluruh karakter cipherteks terkelompokkan.

4. Untuk tiap kelompok karakter, dilakukan analisis frekuensi sehingga dapat diketahui karakter-karakter yang umum muncul untuk setiap kelompok karakter.

5. Karakter hasil analisis tersebut dikumpulkan dan, melalui metode yang serupa dengan dekripsi *Vigenere Cipher*, di"dekripsi" menggunakan "kunci" berupa
    a. Karakter-karakter dengan frekuensi kemunculan tinggi. Sebagai contoh, untuk cipherteks yang teridentifikasi berbahasa inggris dengan kunci teridentifikasi sepanjang 8 karakter, "dekripsi" dilakukan dengan kunci "eeeeeeee" atau;

    b. Rangkaian pola karakter (bigram, trigram, quartogram, dll) yang dikonkatenasi dengan sisa karakter berfrekuensi kemunculan tinggi.

6. "Dekripsi" tersebut akan menghasilkan suatu rangkaian karakter yang dapat diidentifikasi sebagai kunci untuk dekripsi cipherteks. Dekripsi pada cipherteks kemudian dilakukan menggunakan rangkaian karakter tersebut.

Metode Kasiski terbukti mampu memecahkan pesan cipherteks yang dienkripsi menggunakan metode *Vigenere Cipher*. Modal parameter dari pemecahan tersebut hanyalah identifikasi bahasa yang digunakan pada plainteks. Hal tersebut menunjukkan bahwa metode enkripsi ini sudah tidak lagi aman untuk digunakan.

2.3 Pengujian Friedman

Selain Metode Kasiski, pemecahan enkripsi *VIgenere Cipher* dapat juga dilakukan melalui Pengujian Friedman. Pengujian ini dirancang oleh William F Friedman pada tahun 1925. Penerapan matematika mengenai peluang diimplementasikan pada metode ini dalam suatu konsep mengenai *index of coincidence.*

Secara konsep, *index of coincidence* merupakan peluang dua buah karakter yang dipilih secara acak dalam suatu teks adalah sama. Apabila terdapat suatu teks berjumlah N karakter dan diketahui terdapat suatu karakter berjumlah n, maka karakter tersebut memiliki (n/N)x(n/N) peluang terambil dua secara acak.

Dalam penerapan *index of coincidence* pada kriptografi, secara kumulatif, tiap karakter dari 26 alfabet dijumlahkan peluangnya. Hal tersebut akan menghasilkan suatu angka berpola yang dapat menunjukkan bahwa suatu teks adalah cipherteks atau bukan, sekaligus mengidentifikasi bahasa yang digunakan dalam cipherteks tersebut.

Pola angka *index of coincidence* terkait bahasa dapat dilihat pada tabel di bawah ini.

Tabel 1: Angka *index of coincidence* beberapa bahasa di dunia

Bahasa	**IC**
Inggris	0,0667
Rusia	0,0529
Jerman	0,0726
Spanyol	0,0775

Secara matematis, *index of coincidence* dapat dirumuskan sebagai berikut:

$$IC = \frac{\sum_{j=1}^{26} n_j(n_j-1)}{N(N-1)}$$

dalam hal ini, *n* adalah frekuensi karakter ke *i* dalam alfabet dan *N* adalah jumlah karakter dalam sampel. Perlu kita perhatikan bahwa karakter yang terdistribusi secara merata akan menghasilkan perkalian 26 x 1/26 x 1/26 yang menghasilkan angka

0,0385. Hal ini menunjukkan bahwa suatu teks yang dienkripsi tidak mungkin memiliki angka *index of coincidence* di bawah bilangan tersebut.

Dengan diketahuinya pola bahasa yang digunakan dalam suatu cipherteks, metode pemecahan *Vigenere Cipher* semakin mudah. Selain itu, melalui angka *index of coincidence*, serta panjang teks, dapat ditentukan penghitungan untuk mencari panjang kunci *cipher* tersebut.

2.4 *One-time Pad*

Satu-satunya algoritma enkripsi yang diklaim belum dapat dipecahkan adalah algoritma *one-time pad*. Algoritma ini memanfaatkan aspek *Vigenere Cipher* yang diperkuat dengan kunci yang memiliki panjang sama dengan panjang plainteks.

Algoritma ini memiliki kelemahan. Kelemahan yang pertama adalah bahwa kunci yang digunakan sangat panjang dan membutuhkan sumber daya komunikasi dan penyimpanan yang tidak efisien. Kemudian kelemahan yang kedua adalah bahwa kunci yang digunakan hanya aman untuk sekali pakai. Penggunaan kunci kedua kalinya menyebabkan dokumen dapat dengan mudah ditemukan polanya menggunakan metode yang serupa dengan metode pemecahan *Vigenere Cipher* yang telah dijelaskan pada upabab 2.2 dan 2.3.

Akan tetapi, untuk penggunaan yang sesuai, algoritma ini menjamin suatu enkripsi yang tidak mungkin dipecahkan melalui analisis frekuensi dan pengayanya seperti metode kasiski maupun pengujian friedman. Hal tersebut disebabkan pola substitusi karakternya yang acak tanpa pengulangan pola.

3. ENKRIPSI-PEMBANGKIT KUNCI BERGESER

3.1 Definisi

Enkripsi-Pembangkit Kunci Bergeser adalah suatu pengaya dari *Vigenere Cipher* yang memanfaatkan faktor ketiadaan pola pengulangan sebagaimana pada *one-time pad.* Akan tetapi, metode ini tidak membutuhkan sumber daya penyimpanan sebanyak metode *one-time pad*.

Metode ini memperpanjang kunci yang diajukan untuk mengenkripsi plainteks dengan melakukan enkripsi tambahan pada kuncinya. Kunci tersebut di"enkripsi" dengan suatu "kunci" yang merupakan pergeseran *string* kunci sebanyak *i* karakter. Hasil dari enkripsi kunci tersebut dikonkatenasi pada kunci yang lama. Metode tersebut diulangi terhadap bagian tambahan kunci tersebut dengan bagian tambahan sebagai "plainteks" dan pergeseran karakter pada bagian tambahan tersebut sebagai"kunci" baru. Konkatenasi kunci dilakukan hingga kunci memiliki panjang yang sama dengan plainteks.

3.2 Implementasi

Berikut ini adalah penjelasan mengenai implementasi Enkripsi-Pembangkit Kunci Bergeser disertai contoh. Contoh implementasi yang diberikan hanya berupa enkripsi terhadap karakter alfabet.

Plainteks (40 karakter)
mild run in air is an anagram of my lecturers name

Kunci
kidding

Kunci pada contoh tersebut akan diperpanjang menggunakan Enkripsi-Pembangkit Kunci Bergeser

Kunci dummy: kidding <<
iddingk
K-Enkripsi: slglvtq
Konkatenasi: kiddingslglvtq….

Kunci Akhir
kiddingslglvtqdrrgojiuixuxrlcfrrocfhwifq

Cipherteks
wqogzhtaygtmbidertopzuulzjpwghklfgwzjiru

Melalui contoh tersebut, dapat kita perhatikan bahwa metode enkripsi ini memungkinkan beberapa parameter masukan lainnya seperti jumlah dan arah pergeseran dari generator kunci. Berikut adalah contoh lain dengan masukan tambahan berupa kedua parameter tersebut.

Plainteks (40 karakter)
mild run in air is an anagram of my lecturers name

Kunci
kidding

Arah geser: kanan
Jumlah geser: 2

Kunci dummy: kidding<<2
ngkiddi
K-Enkripsi: xonllqo
Konkatenasi: kiddingxonllqo….

Kunci Akhir
kiddingxonllqonckzybzobxbiaxoylcfbfpdzaqdk

Cipherteks
wqogzhtfbntcygnpkmyhqonlguyisaewwfwhqzmu

3.3 Analisis

Pada dasarnya, metode enkripsi ini menerapkan prinsip pengacakan pola sebagaimana yang dapat dikaji dari pola *one time pad.* Pengacakan tersebut memungkinkan sulitnya dilakukan analisis frekuensi sekalipun diperkaya dengan Metode Kasiski. Ketidakmungkinan dilakukannya pemecahan dengan Metode Kasiski disebabkan tidak adanya pola berulang yang menentukan panjang kunci. Pengujian Friedman pun dapat dikatakan tidak berdaya untuk melakukan pengkajian *index of coincidence* karena karakter-karakter yang terenkripsi tidak dapat ditentukan sebagai satu pola pengulangan substitusi.

Hal lain yang perlu diperhatikan adalah bahwa metode enkripsi ini tidak memerlukan besar kunci yang membutuhkan sumber daya memori maupun komunikasi yang kompleks. Selain itu, kunci yang menjadi syarat utama terpecahkannya cipherteks tersebut dapat dipisahkan menjadi tiga unsur, yaitu teks kunci itu sendiri, jumlah, dan arah pergeseran. Ketiga unsur kunci tersebut dapat dikirim secara terpisah sehingga meminimalisasi terpecahkannya cipherteks akibat intersepsi komunikasi kunci.

4. KESIMPULAN DAN SARAN

Modifikasi *Vigenere Cipher* menggunakan Enkripsi-Pembangkit Kunci Bergeser mampu memperkuat kualitas cipherteks dalam hal keamanan dengan adanya faktor pengacakan pola. Di sisi lain, metode ini tidak membutuhkan sumber daya memori yang besar sebagaimana *one-time pad*. Keunggulan lainnya berada pada kunci yang memiliki tiga unsur yang dapat dipisahkan baik dalam hal penyimpanan maupun pendistribusiannya. Hal ini meningkatkan faktor keamanan yang mampu didukung secara fungsional melalui metode ini.

Adapun mengenai peningkatan kualitas keamanan, salah satu hal yang dapat dimodifikasi lebih lanjut adalah dengan melakukan pencerminan *string* kunci sebelum dilakukannya K-Enkripsi. Hal tersebut dilakukan untuk menambah faktor acak yang didukung metode ini dalam pengamanan pola cipherteks.

DAFTAR PUSTAKA

Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

www.bbc.co.uk/dna/h2g2/alabaster/A613135.html
tanggal akses: 23 Maret 2010

http://home.att.net/~tleary/cryptolo.htm
tanggal akses: 23 Maret 2010

http://www-math.cudenver.edu/~wcherowi/courses/m5410/m5410cc.html
tanggal akses: 23 Maret 2010

http://www.ranum.com/security/computer_security/papers/otp-faq/
tanggal akses: 23 Maret 2010