

# BACON'S CIPHER

Aloysius Adrian – NIM : 13506031

Program Studi Teknik Informatika, Institut Teknologi Bandung

Jl. Ganesha 10, Bandung

E-mail : [if16031@students.if.itb.ac.id](mailto:if16031@students.if.itb.ac.id)

## Abstrak

Steganografi adalah teknik untuk menyembunyikan pesan dengan cara menyamarkannya ke dalam pesan lainnya. Berbeda dengan kriptografi yang dengan sengaja mengubah pesan menjadi pesan cipher yang tidak terbaca, steganografi menyembunyikan pesan di dalam pesan lain namun pesan lain ini tetap dapat dibaca dan memiliki arti juga. Bacon's cipher merupakan salah satu teknik steganografi yang klasik, kuno, unik, namun tidak terlalu umum diketahui orang. Walaupun namanya menyiratkan kriptografi (cipher), namun Bacon's cipher merupakan teknik steganografi. Bacon's cipher diciptakan oleh Sir Francis Bacon pada sekitar abad 16. Namun keberadaannya serta pembahasannya baru mencuat pada akhir abad 19. Bacon's cipher telah menyembunyikan banyak rahasia pada masanya. Beberapa rahasia yang terkuak akan dibahas dalam makalah ini. Dalam makalah ini akan dibahas pula teknik dasar steganografi Bacon's cipher beserta beberapa variasi yang membuat Bacon's cipher menjadi sebuah teknik steganografi yang unik dan patut dikaji.

**Kata Kunci** : Bacon's cipher, steganografi, kriptografi, Shakespeare

## 1. Pendahuluan

Sir Francis Bacon hidup dari tahun 1561 hingga 1626 tetapi beberapa kalangan percaya bahwa beliau masih tetap hidup melebihi tahun 1626 dengan mengganti namanya dan pindah menetap ke Jerman. Bacon adalah seorang Inggris dan dipercaya juga bahwa beliau merupakan anak tidak sah dari Queen Elizabeth.



**Gambar 1** Sir Francis Bacon

Selama selang waktu hidupnya, Bacon telah menciptakan banyak karya yang jauh melampaui teknologi di jamannya. Salah satunya adalah teknik steganografi ini. Bacon mempelajari penggunaan cipher sejak masa mudanya saat dia dipekerjakan oleh Lord Burghley dan Sir Francis Walsingham di bawah kekuasaan Ratu Inggris. Bacon tidak hanya menggunakan cipher tapi juga menemukan beberapa cipher sendiri. Salah satunya beliau deskripsikan dalam *De Augmentis Scientiarum*, pertama kali dipublikasikan dalam translasi Inggris tahun 1640. Cipher tersebut diberi nama *biliteral cipher*, yang disebutkan bahwa Bacon temukan pada masa mudanya di Paris tahun 1576 – 1579. Dari biliteral cipher ini, lahirlah teknik dasar kode Morse yang kemudian dikembangkan, dan juga sistem biner yang digunakan komputer – komputer masa kini.

Contoh karya beliau yang lain adalah mahakarya literatur Inggris yang diciptakan Shakespeare ternyata merupakan karya Sir Francis Bacon. Sungguh mencengangkan untuk menemukan pesan rahasia yang disembunyikan dengan steganografi pada naskah asli dari karya Shakespeare. Beberapa isinya adalah *signature* beliau bertuliskan namanya (*bacon, becen, baecen, baicyn*, dan lain – lain). Terdapat pula bukti kuat yang berisikan “*Francis Bacon wrote Shakespeare's plays*” yang ditemukan pada *Shakespeare's funerary monument*. Monumen tersebut mengandung tulisan dalam biliteral. Sayangnya, monumen ini telah sering diperbaiki sehingga banyak bagian yang diperbaiki ini menghilangkan sebagian tulisan aslinya.



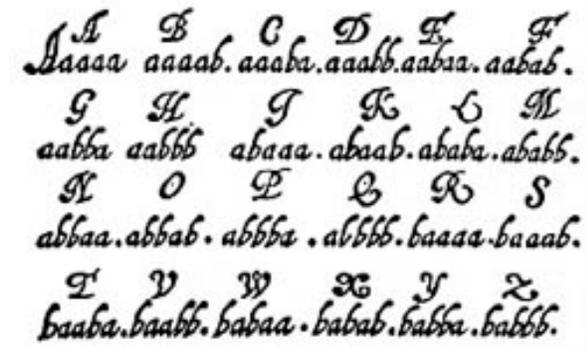
Gambar 2 Disk cipher salah satu teknik kriptografi temuan Bacon

## 2. Teknik Steganografi pada Bacon's Cipher

Pada dasarnya, teknik steganografi menggunakan Bacon's cipher tidaklah terlalu rumit. Teknik steganografi menggunakan cara baconian berpusat pada tabel di bawah ini.

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

Tabel 1 Konversi alfabetik pada Bacon's Cipher



Gambar 3 Naskah saduran asli tentang konversi alfabetik pada Bacon's Cipher

Dapat dilihat bahwa korespondensi dari huruf – huruf di sebelah kiri kolom (a, b, c, ...) dengan kelompok huruf di sebelah kanan kolom tidak terlalu menjelaskan apa makna Bacon's cipher. Tabel di atas akan lebih mudah dipahami bila dalam bentuk bilangan biner seperti yang tergambarkan pada tabel di bawah ini. Tabel berikut adalah tabel yang digunakan pada variasi Bacon's cipher.

a	00000	g	00110	n	01100	t	10010
b	00001	h	00111	o	01101	u-v	10011
c	00010	i-j	01000	p	01110	w	10100
d	00011	k	01001	q	01111	x	10101
e	00100	l	01010	r	10000	y	10110
f	00101	m	01011	s	10001	z	10111

Tabel 2 Tabel konversi alfabet ke biner pada Bacon's Cipher

Dasar dari steganografi ini adalah dengan menggantikan atau melambangkan sebuah alfabet dengan sebuah deretan huruf yang dapat juga dianalogikan dengan bilangan biner 0 dan 1. Satu kelompok bilangan biner yang terdiri dari 5 digit angka ini akan merepresentasikan bagaimana huruf akan digambarkan, apakah huruf kapital atau huruf kecil.

### 2.1 Aplikasi Bacon's Cipher

Anggap saja kita memiliki sebuah kalimat : “dia tidak berlari” dan di baliknya kita akan menyembunyikan sebuah kata misalnya : “anu”.

Kata “anu” bila dicoba ditranslasikan menggunakan bacon's table versi biner akan menjadi :

A : 00000

N : 01100

U : 10011 (di sini terlihat U dan V berbenturan pada tabel)

Rangkaian angka biner tersebut akan menjadi 000000110010011. Dari deretan angka berikut inilah kalimat “dia tidak berlari” akan dimodifikasi. Proses modifikasinya sendiri dapat dikatakan tidak rumit. Cukup menggantikan huruf yang berkorespondensi dengan angka biner 0 dengan huruf kecil dan angka 1 dengan huruf kapital. Hasil translasi kalimat akan menjadi : “diatidAKbeRlaRI”

Teknik steganografi di atas merupakan metode pertama dalam Bacon's cipher. Teknik penulisan dengan percampuran huruf kapital dan huruf kecil disebut *bilateral writing*.

Contoh lain dalam steganografi dengan teknik Bacon sebagai berikut.

Plain Teks : ITS BACON

Cipher Teks : abaaa baaba baaab aaaab aaaaa aaaba abbab abab

Cipher teks sudah siap untuk diubah ke cover teks. Cara pertama telah diperlihatkan tadi, berikut ini adalah teknik kedua dari Bacon's Cipher. Diasumsikan, seluruh huruf dari "A" hingga "K" akan diubah menjadi "a" dan sisanya diubah menjadi "b" lalu kita dapat mengubah Encoded teks menjadi cover teks sebagai berikut.

Et: a baaa baa bab aaa ba aaa baa aaa aaab abab baba babb

Ct2: I like the new bag. We had the bag kids get Nana less.

Dapat terlihat bahwa contoh ini merupakan cara paling aman untuk menyembunyikan plain teks di balik cover teks karena pemilihan kata lebih dinamis dan tidak terbatas.

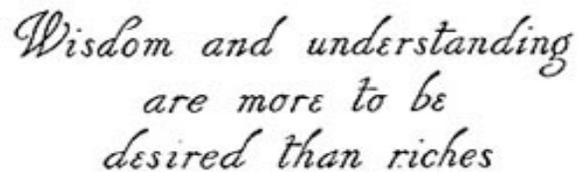
Pada contoh Bacon's cipher pertama, mungkin timbul pertanyaan. Cover teksnya akan menjadi mencurigakan bila ditulis dengan tipografi yang berbeda - beda (huruf kapital dan huruf kecil). Bacon tentu saja menemukan sebuah cara untuk membuat coverteks tidak mencurigakan dengan menciptakan tipografi sendiri untuk digunakan. Contoh gambar tipografi temuan Bacon



Gambar 4 Biliteral Writing Temuan Bacon

Tipografi *bilateral writing* di atas diambil dari karya Bacon *De Augmentis Scientiarum*.

Contoh penggunaan Bacon's cipher pada masa lalu



Gambar 5 Contoh penulisan menggunakan biliteral writing

Teks di atas merupakan contoh *bilateral writing* yang mendasari teknik Bacon's cipher. Pada teks di atas terdapat perbedaan penulisan huruf "d" pada kata "wisdom" dan "and", "i" pada "wisdom" dan "understanding", 2 huruf "e" pada "desired", "o" pada "more" dan "wisdom", "r" pada "more" dan "understanding", "a" pada "than" dan "are"

Contoh lain paragraf yang ditulis secara biliteral

*Ego omni officio, ac potius pietate erga te. ceteris satisfacio omnibus: Mihi ipse nunquam satisfacio. Tanta est enim magnitudo tuorum erga me meritorum, ut quoniam tu, nisi perfecta re, de me non conquiesci; ego, quia non idem in tua causa officio, vitam mihi esse acerbum putem. In causa haec sunt: Ammonius Regis legatus aperte pecuniam nos oppugnat. Res agitur per eosdem creditores, per quos, cum tu aderans, agebatur. Regis causa, si qui sunt, qui velint, qui pauci sunt, omnes ad Pompeium rem deferri volunt. Senatus Religionis calumniam, non religionem, sed maiestatem, et illius Regiae Cognitionis invidia comprobatur. &c.*

Gambar 6 Contoh lain penulisan menggunakan biliteral writing

Teknik berikutnya dalam Bacon's cipher adalah dengan teknik ini, yang diperhatikan adalah huruf vokal dan konsonan. Misalnya pada contoh berikut ini :

LADieS aND GENTlEMEn, thANK YOU FoR  
COmIng hErE

Dengan mengelompokkan seluruh huruf kapital menjadi

LADSN DGENE MEANK YOUFR COIEE

Lalu mengubah seluruh huruf vokal menjadi 1 dan huruf konsonan menjadi 0 dengan hasil

01000, 00101, 01100, 01100, 01111

Bila bilangan biner di atas diubah menjadi bilangan desimal, maka didapatkan

8, 5, 12, 12, 15

Bila angka di atas diubah ke alfabet sesuai urutan, maka di dapat sebuah kata yang disembunyikan yakni HELLO

Cover teks (cipher teks) dari Bacon's cipher terkadang terkesan dibuat - buat. Kadang arti dari cover teks tidak terlalu baik untuk menjadi sebuah paragraf. Akan lebih baik bila pengerjaan Bacon's cipher dilakukan mundur, atau mula - mula ciptakan dahulu cover teksnya dan mengembangkan kata plain teks dari sana.

Terdapat beberapa sugesti, Kita dapat membuat banyak enkripsi yang berbeda - beda berdasarkan Baconian cipher. Kunci dari cipher - cipher demikian adalah ukuran dari waktu mengenkoding dikalikan ukuran fungsi dari Encoded teks ke Cipher Teks.

|Baconian Encodings| = P(32, 24)

26!

|f:Et->Ct2| = -----

11115!

## 2.2 Variasi dalam Bacon's Cipher

Terdapat tiga variasi dalam Bacon's cipher. Simple cipher, Reverse cipher, dan Kay cipher. Terdapat dua variasi Kay cipher, namun yang akan dibahas dan lebih sering digunakan (bahkan digunakan dalam Shakespeare Folio of Plays) adalah versi kedua.

### 2.2.1 Simple Cipher

Teknik paling sederhana dari Simple cipher adalah dengan memberi nomor urutan pada 24 karakter Bacon.

A	1
B	2
C	3
...	
I	9

K	10
L	11
...	
S	18
T	19
V	20
W	21
X	22
Y	23
Z	24

**Tabel 3 Pengurutan pada simple cipher**

Simple cipher, atau Bacon menyebutnya *four-fold structure*, dikembangkan oleh Bacon dengan mengulangi 24 huruf sebanyak 4 kali sehingga nomor urutan mencapai 96 (4 X 24) dan masing – masing nomor/ huruf pada 4 kelompok ini mengacu pada huruf alfabetik.

Simple cipher diilustrasikan dalam buku yang dibuat oleh Gustavus Selenus, *Cryptomenitices et Cryptogaphiae*, yang diterbitkan di Jerman tahun 1624.

### 2.2.2 Reverse Cipher

Variasi kedua adalah Reverse cipher. Reverse cipher pada dasarnya adalah Simple cipher dengan urutan huruf terbalik. Reverse cipher dimaksudkan untuk memeriksa silang naskah Bacon's cipher karena seringkali Bacon's menyembunyikan kata dengan urutan terbalik.

A	24
B	23
C	22
...	
I	16
K	15
L	14
...	
S	7
T	6
V	5
W	4
X	3
Y	2
Z	1

**Tabel 4 Pengurutan pada Reverse cipher**

### 2.2.3 Kay Cipher

Variasi ketiga adalah Kay Cipher. Kay cipher pertama dibicarakan oleh Francis Bacon pada versi tahun 1605 dari bukunya yang berjudul *Advancement of Learning*, namun tidak dibahas. Dalam buku *De Augmentis Scientiarum* versi latin tahun 1623, Bacon menyebut Kay cipher sebagai "Ciphrae Clavis" (Key Ciphers). Pada akhirnya, Kay cipher berhasil diencode oleh W.E.Clifton dengan bantuan buku Rawley's *Resuscitatio* (1671) dan Thomas Powell's *The Repertoire of Records* (1631). Clifton menemukan bahwa pada Kay cipher digunakan 26 karakter. 24 Karakter dalam simple cipher ditambah dengan karakter "&" dan kata "et". Ditambah lagi, pada Kay cipher, pengurutan dimulai dari huruf "K" dengan urutan awal "K" adalah 10. Karena karakter pada urutan 25 dan 26 (merupakan karakter "&" dan "et") diperlakukan sebagai karakter null, maka "A" menjadi urutan 27, "B" urutan 28 dan seterusnya.

A	27
B	28
C	29
D	30
E	31
F	32
G	33
H	34
I	35
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
V	20
W	21
X	22
Y	23
Z	24

**Tabel 5 Pengurutan pada Kay Cipher**

### 2.3 Penn Leary's Baconian Cipher

Prinsip utama pada Bacon's cipher versi leary berdasar pada 21 huruf alfabet : "ABCDEFGHIJKLMNOPQRSTUVWXYZ".

Urutan alfabet ini tidak mengikutsertakan huruf "JUWXZ" karena pada jaman Elizabethan huruf "I" dan "J" sering digunakan bertukar - tukaran, seperti juga pada huruf "U" dan "V" serta "W" yang sering ditulis sebagai "VV". Huruf "X" dan "Z" dihilangkan karena bangsa Romawi tidak memakai alfabet ini. Hal ini menjelaskan mengapa tabel enkripsi Bacon's cipher mengandung 2 huruf untuk 1 kode. Berdasarkan 21 alfabet Bacon's ini, Leary percaya bahwa Bacon menggeser masing - masing huruf dengan huruf ke 4 setelahnya. "A" menjadi "E" dan seterusnya.

ABCDEF GHIKLMNOPQRSTVY  
e f g h I k l m n o p q r s t v y a b c d

Pada masa ini, belum dibuat standar baku dalam pengejaan kata. Ada banyak cara untuk mengeja Shakespeare, begitu pula mengeja Bacon. Ada yang menggunakan Bacen untuk mengeja dan lain - lain. Penn Leary telah menemukan banyak tanda tangan Bacon dalam karya - karya Shakespeare. Berikut adalah daftar kemunculan nama Bacon dalam berbagai versi penulisan dan berbagai literatur Inggris lainnya (tidak hanya karya Shakespeare).

Naskah	X kemunculan nama Bacon
Arte of English Poesie	192
Spenser's Faerie Queene	548
Caesar's Galiic Wars	64
Longfellow's Song of Hiawatha	327
Burrough's Tarzan of the Apes	135
Melville's Moby Dick	347
Federalist Papers	239
Senate Majority Whitepaper Report	396

**Tabel 6 Daftar kemunculan tandatangan Bacon pada beberapa literatur Inggris**

### 3. Kesimpulan

Pada masanya, Bacon's cipher tidak dapat dipecahkan dengan mudah. Tidak banyak orang yang tahu tentang keberadaan Bacon's cipher selain orang - orang pengikut sekte Baconian. Pada dasarnya, steganografi dengan Bacon's cipher ini digunakan oleh sekte Baconian untuk bertukar informasi tanpa diketahui orang biasa. Hingga akhirnya mulai bermunculan buku - buku yang mulai mebeberkan dan memberikan pembahasan mengenai teknik yang

digunakan dalam Bacon's cipher, khalayak umum mulai menyadari betapa banyaknya karya atau naskah yang ternyata di dalamnya terkandung pesan rahasia.

Pada masa sekarang ini, pembahasan mengenai sejarah hidup Sir Francis Bacon, teknik steganografi Bacon's cipher, dan naskah - naskah rahasia menjadi pembahasan yang sangat menarik. Walaupun mungkin tidak mudah lagi untuk menyembunyikan pesan menggunakan teknik Bacon's cipher, tapi tetap saja tidak banyak orang yang tahu tentang teknik Bacon's cipher.

### Daftar Pustaka

- [1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.
- [2] <http://www.prs.org> tanggal akses 25 Maret 2009
- [3] <http://home.att.net/~tleary/mainmenu.htm> tanggal akses 25 Maret 2009
- [4] <http://www.purplehell.com/riddletools/bacon.htm> tanggal akses 25 Maret 2009 - merupakan tool online untuk membuat stegaografi Bacon's cipher sederhana.
- [5] <http://shakespeareauthorship.com> tanggal akses 25 Maret 2009