Djamijah Cipher: Memori Vigenère dari Pacitan

Agung Prabowo

Selama berabad-abad, para raja, ratu dan jenderal membangun komunikasi efektif dengan tujuan mempermudah pengaturan dan pengelolaan wilayah bawahan dan memberi perintah atau komando kepada para tentaranya. Mereka tidak ingin pesan-pesan yang dikirimkan jatuh ke tangan musuh. Oleh karena itu, dikembangkan metode pembuatan pesan sehingga hanya penerima yang dituju yang dapat membaca pesan tersebut.

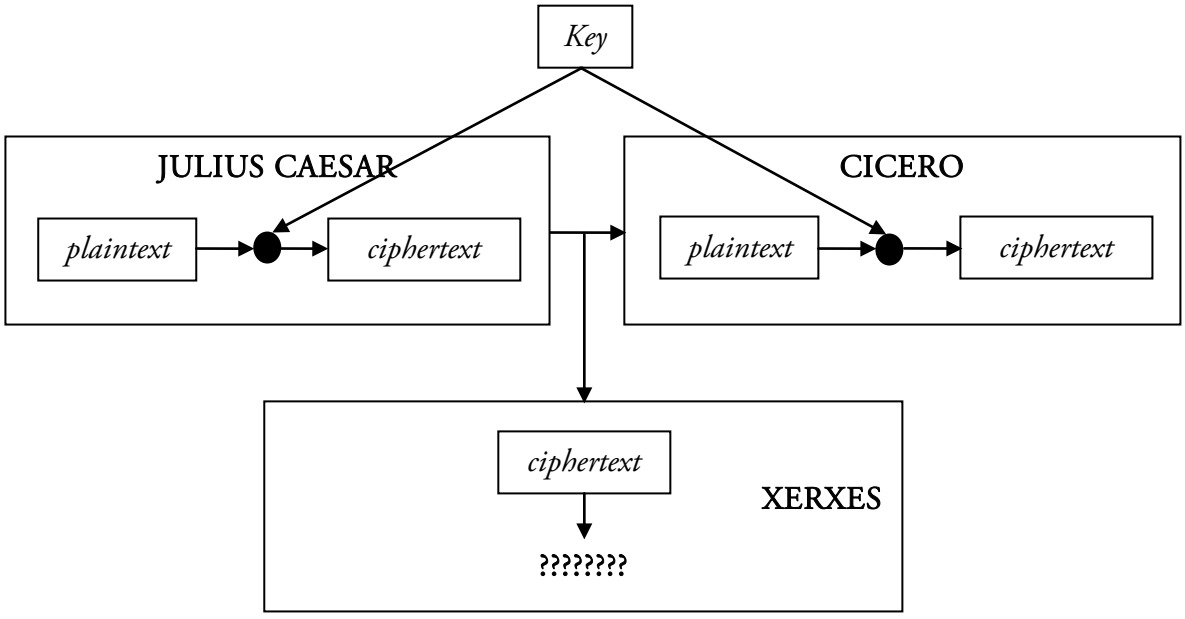
Kriptografi dan kriptoanalisis ibarat sekeping mata uang. Dalam kriptografi terlibat dua pihak yaitu pembuat (pengirim) pesan asli dan penerima (pembaca) pesan terkirim tersebut. Pesan asli yang dapat langsung dibaca akan diistilahkan dengan *plaintext* sedang pesan terkirim atau pesan rahasia yang telah disandikan akan disebut *ciphertext*. Dalam kriptografi, kedua pihak tersebut sebelumnya sudah sepakat dengan satu kata kunci yang sama sehingga keduanya tidak mengalami kesulitan dalam komunikasi melalui pesan rahasia tersebut. Dalam kriptoanalisis muncul pihak ketiga yang sebenarnya tidak terlibat dalam proses komunikasi namun karena memperoleh pesan rahasia (baik sengaja maupun tidak), pihak ketiga ini menjadi berkepentingan untuk memecahkan pesan tersebut dan mengorek informasi yang dikandungnya. Pihak ketiga tentu saja tidak punya kunci sehingga ia harus berusaha menemukan kunci tersebut agar pesan rahasia yang diperolehnya dapat dipecahkan. Pencarian kunci menjadi kajian dalam bidang kriptoanalisis.

Dalam tulisan ini, posisi kita adalah sebagai pihak ketiga yaitu pihak yang secara kebetulan mempunyai pesan rahasia namun tidak punya

kunci untuk memecahkannya. Frase 'secara kebetulan' dimunculkan karena sebenarnya kita tidak punya kepentingan dengan informasi yang terkandung dalam pesan rahasia ini. Sebagai pihak ketiga, kita tidak bermaksud untuk mencari dan menemukan kunci dari pesan tersebut. Artinya, tulisan ini tidak akan memasuki wilayah kriptoanalisis. Seseorang (yaitu Mr. J.W. Stumpel) telah menemukan kuncinya seperempat abad yang lalu dan posisi kita dalam hal ini hanyalah sebagai pihak yang sedikit banyak memperoleh pengetahuan baru tentang matematika kolonial di Nusantara.

Pembuat atau pengirim pesan rahasia tersebut menggunakan inisial rahasia G.B.F.F.Q.S. Lantas, siapakah orang yang dituju sebagai penerima pesan rahasia tersebut? Menurut hemat kami, penerima pesan ini tidaklah terdefinisi dengan jelas. Mungkin pembuat pesan sama sekali tidak ingin diketahui siapa dirinya. Bisa jadi pula pesan rahasia ini justru ditujukan untuk para matematikawan atau kriptografer yang secara sengaja atau tidak menemukannya. Mungkinkah pesan rahasia ini ditujukan kepada seseorang yang sangat dicintai oleh pengirim pesan, sebagai sebentuk doa? Kemungkinan lainnya adalah pesan rahasia ini ditujukan kepada keturunan pembuat atau pengirim pesan. Sampai saat ini, tidak diketahui dengan pasti siapakah orang yang mempunyai kunci untuk membaca pesan tersebut, kecuali mungkin perancang pesan tersebut jika bukan G.B.F.F.Q.S. sendiri yang merancangnya.

Gambar 1 memperlihatkan skema umum dari suatu kriptografi. Misalkan dua pihak yang akan berkomunikasi (secara rahasia) adalah Julius Caesar dan Cicero, filosof dan sastrawan Romawi. Julius Caesar mengirimkan suatu pesan rahasia kepada Cicero. Sangat mungkin bahwa pesan yang dirimkan Julius Caesar tidak sampai kepada Cicero, tetapi jatuh pada pihak ketiga (musuh), dalam hal ini adalah Xerxes, Kaisar Persia. Agar pesan tersebut tidak dapat dibaca oleh Xerxes, maka Julius Caesar harus



Gambar 1. Skema Kriptografi

menulisnya dalam bentuk pesan rahasia atau pesan yang disandikan yang disebut *ciphertext*.

Baik Julius Caesar maupun Cicero keduanya mempunyai kunci (*key*) yang dapat digunakan untuk membuat atau memecahkan pesan tersebut (*ciphertext*), sementara Xerxes tidak mempunyai kunci yang dimiliki oleh Julius Caesar dan Cicero. Apabila pesan yang disandikan tersebut jatuh ke tangan Xerxes, maka diharapkan Xerxes tidak dapat membacanya, kecuali Xerxes berhasil menemukan kunci tersebut.

Untuk menghasilkan pesan rahasia, maka Julius Caesar harus melakukan enskripsi yaitu proses merubah pesan asli (*plaintext*) menjadi pesan yang disandikan atau pesan terkirim (*ciphertext*). Proses kebalikannya disebut dekripsi dan akan dilakukan oleh Cicero sesaat setelah ia menerima pesan yang dikirim Julius Caesar. Hasil dari dekripsi adalah pesan asli. Pihak ketiga yaitu Xerxes juga berusaha melakukan proses dekripsi seperti yang dilakukan oleh Cicero, namun Xerxes harus mampu menemukan kuncinya terlebih dahulu.

Pacitan, 1901

> *Ia yang telah menempuh jauh perjalanan, pada akhirnya jatuh cinta pada kesunyian, memilih tinggal di Pacitan nan sepi. Segera saja, sekonyong-konyong segalanya menjadi lebih sunyi, sunyi yang teramat sangat, sunyi yang nyata, sunyi yang paling sepi hingga akhirnya terpahatlah rasa abadi pada batu epitaf.*

Pacitan, saat ini adalah kota kecil yang masuk dalam Propinsi Jawa Timur. Di kota ini, mantan presiden kita, Susilo Bambang Yudhoyono (SBY) lahir dan tumbuh besar sebelum akhirnya digembleng di Magelang sebagai prajurit TNI AD. Mungkin saja di masa mudanya SBY pernah mengunjungi tenpat yang dimaksudkan dalam tulisan ini, sebuah tempat yang mengawetkan pesan rahasia penuh romantisme.

Pacitan, sekitar 115 tahun yang lalu. Marilah kita bawa memori ke kota kecil tersebut, meskipun saat itu tidak satupun dari kita yang sudah lahir pada saat peristiwa ini terjadi. Saat itu, ide tentang Indonesia belum ada sama sekali. Penyambung Lidah Rakyat, Soekarno, lahir belum lama berselang di tetangga kota, sekitar enam bulan sebelumnya dari suatu tanggal tertentu yang ternukil dalam pesan rahasia ini.

Saat itu, pemerintah kolonial Belanda sedang kuat-kuatnya mencengkeram Nusantara. Nusantara yang *gemah ripah loh jinawi karta raharja*, hampir seluruh kemakmurannya diangkut, dipindahkan dan dinikmati oleh orang-orang di seberang lautan, di negeri Kincir Angin yang identik dengan warna oranye namun berbendera Merah Putih Biru. Seluruh pemberontakan yang muncul di seluruh Nusantara belum lama berselang berhasil ditumpas dengan meyakinkan. Diponegoro telah lama dikalahkan, dan Imam Bonjol mendekati kekalahan. Tanah-tanah di

Nusantara dibuka untuk berbagai jenis perkebunan dengan komoditas yang saat itu laku keras di Eropa. Saat rempah-rempah asal Maluku tidak lagi bernilai tinggi seperti pada abad 15-18 Masehi, perkebunan teh, kopi, kina, tebu terhampar luas pada bentang alam tanah-tanah Nusantara. Berbagai jenis pertambangan juga telah dibuka: minyak bumi, nikel, aspal, tembaga, emas menyebabkan pundi-pundi keuangan kolonial Belanda bertambah banyak.

Pada saat itu, sebuah peristiwa kecil yang sangat tidak penting terjadi di kota Pacitan. Secara politik, peristiwa ini tidak bermakna dan saking tidak pentingnya maka peristiwa tersebut tidak akan pernah direkam dalam sejarah Indonesia ataupun sejarah kolonial Belanda. Namun, peristiwa kecil yang bersifat sangat personal ini menjadi menarik karena kandungan ilmiahnya. Peristiwa ini juga menjadi monumen bukti adanya peninggalan kolonial yang mengawetkan pengetahuan matematika, khususnya matematika persandian.

Peran kami dalam peristiwa ini hanyalah penyampai kepada siapa saja yang mempunyai ketertarikan untuk melakukan studi kripto-analisis guna menemukan cara berbeda dalam memperoleh kunci dan memecahkan sandi rahasia ini. Tidak ada kebaruan yang bisa kami munculkan dalam tulisan ini, namun tulisan ini memberikan kepada kita pengetahuan bahwa sebelum kita belajar matematika yang hari ini dipelajari di seluruh dunia, monumen dari Pacitan ini telah menjadi bukti adanya matematika (persandian) di Nusantara yang merupakan peninggalan kolonial.

Siapa sangka jika sebuah nisan atau pusara mengawetkan pengetahuan matematika. Sesungguhnya, fakta tersebut tidaklah terlalu aneh. Pahatan-pahatan pada batu yang saat ini disebut Plimpton 322 menuangkan pengetahuan matematika yang sekarang dikenal sebagai Tripel Babilonia dan dikembangkan dalam buku *The Elements* karya Euclid menjadi Tripel Pythagoras. Saat ini kita mengenalnya sebagai Teorema/Dalil Pythagoras.

Pada sebuah pusara, yang dibawahnya bersemayam wanita yang mati pada muda usia (1873 – 1901), mengguratkan 26 baris sandi yang tergolong dalam Sandi Vigenère. Salah satu cabang matematika yang membahas Sandi Vigenère ini adalah Teori Bilangan. Kita dapat menemukan pada Bab 10: *Introduction to Cryptography* dalam buku *Elementary Number Theory* karya David M. Burton. Cameron (2003) menyebutkan kriptografi sebagai bagian dari Teori Komunikasi yang disebut Teori Koding.

Bentuk sandi Vigenère pertama kali tercatat dalam *Traicté de Chiffres* yang dipublikasikan oleh kriptografer Perancis, Blaise de Vigenère (1523-1596) pada tahun 1586. Nama penemunya pada akhirnya dilekatkan sebagai nama sandi yang ditemukannya. Sandi Vigenère merupakan pengembangan dari Kaisar (*Caesar cipher*).

Laporan pertama kali tentang penggunaan Sandi Kaisar muncul dalam Perang Galia (*Gallic Wars*), lebih dari 2000 tahun yang lalu. Kata 'kaisar' dalam Sandi Kaisar merujuk pada salah seorang kaisar Romawi yang sangat termashur, *Julius Caesar*, yang juga berjasa dalam merevisi

kalender matahari bangsa Mesir Kuno menjadi Kalender Julian yang masih digunakan hingga 4 Oktober 1582.

Ide dasar dalam Sandi Kaisar adalah substitusi. Setiap huruf yang membentuk rangkaian persandian digantikan (disubstitusi) dengan huruf tertentu berdasarkan aturan dasar yang sama. Aturan dasar tersebut adalah menggeser setiap huruf sejauh tempat tertentu ke sebelah kanan. Pada umumnya, *Julius Caesar* menggunakan pergeseran tiga tempat ke sebelah kanan dalam siklus aksara yang memuat huruf A, B, ..., Z sehingga setelah huruf Z akan kembali lagi ke huruf A. Sandi Kaisar mempunyai 25 kunci yang mungkin.

Dalam tulisan ini, pesan asli (*plaintext*) akan dituliskan dengan huruf kecil, sedangkan pesan terkirim (*ciphertext*) akan ditulis dengan huruf besar. Sebagai contoh, untuk mengirim pesan asli yang berbunyi "Saya akan pulang lusa" maka *Julius Caesar* akan menuliskannya dengan XFDF FPFS UZQFSL QZXF, menggunakan pergeseran lima tempat ke kanan.

Saya akan pulang lusa

XFDF FPFS UZQFSL QZXF

Contoh ini dapat kita lihat pada tulisan populer "Matematika Persandian" karya Hendra Gunawan. Dalam contoh ini, kita katakan *Julius Caesar* menggunakan Kunci *v* sebab huruf *v* pada pesan asli akan disandikan menjadi huruf A pada pesan terkirim. Dengan kata lain, dengan Kunci *v* maka huruf *v* disandikan menjadi A. Selanjutnya, Sandi Kaisar dengan Kunci *v* akan menyandikan A menjadi F, B menjadi G, dan seterusnya (Gambar 2). Penggunaan Kunci *v* ini menjadi sering karena kekuatan magisnya yang mengasosiakan huruf *v* dengan kata *victory* (kemenangan sempurna).

Plain text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher text	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Gambar 2. Kunci *v* dalam Sandi Kaisar

Secara matematis, Sandi Kaisar akan membentuk sebuah grup (Cameron, 2003). Jika dalam sistem aksara (alfabet) $A = \{a_0, a_1, ..., a_{q-1}\}$ maka pergeseran sejauh i tempat dapat ditulis dengan $f_i : a_j \mapsto a_{j+i \bmod q}$ dengan orde *q*. Selanjutnya, kita punya hasil:

$$f_{i_1} \circ f_{i_2} = f_{i_1+i_2 \bmod q}$$

$$f_0 = e$$

$$f_i^{'} = f_{-i \bmod q}$$

Untuk contoh di atas, penyandian membentuk sebuah grup dengan orde $q = 26$ dan dengan Kunci *v* maka $f_5 : a_j \mapsto a_{j+5 \bmod 26}$. Dalam Kunci *v*, $f_0 = e = v$. Penerima pesan akan membaca pesan dengan cara kebalikannya yaitu menggeser setiap huruf lima langkah ke belakang berdasarkan $f_5^{'} = f_{-5 \bmod 26}$.

Beberapa ahli menamakan substitusi pada Gambar 1 sebagai Kunci *F* sebab huruf a pada pesan asli (*plaintext*) akan disandikan menjadi huruf F pada pesan terkirim (*ciphertext*). Ini artinya, dengan Kunci *F* maka huruf F menyandikan huruf a. Dengan demikian, akan ada dua cara penamaan kunci, pertama

berdasarkan huruf pada *plaintext* (Kunci *v*: $v \mapsto A$) dan yang kedua berdasarkan huruf pada *ciphertext* (Kunci *F*: $a \mapsto F$).

Dalam Sandi Kaisar, menggeser 25 langkah ke kanan akan menyandikan huruf A menjadi Z. Sementara itu, menggeser 1 langkah ke kiri juga akan menyandikan huruf A menjadi Z. Akibatnya, $f_{25} : a_j \mapsto a_{j+25 \bmod 26}$ akan ekuivalen dengan $f_{-1} : a_j \mapsto a_{j-1 \bmod 26}$.

Sandi Kaisar sangat mudah dipecahkan, meskipun kita tidak mengetahui kunci yang digunakan untuk menyandikannya. Dalam Sandi Kaisar hanya ada 26 buah kunci sesuai jumlah huruf dalam sistem aksara (alfabet) yang digunakan dalam pembuatan Sandi Kaisar, namun satu kunci akan menghasilkan *ciphertext* yang tepat sama dengan *plaintext*. Dengan mencobakan satu per satu dari dua puluh lima kunci tersebut, maka Sandi Kaisar akan terpecahkan. Contoh penggunaan Sandi Kaisar dalam era modern dapat ditemukan dalam fiksi-sains karya Arthur C. Clarke berjudul *2001: A Space Odyssey* yang memberi nama sebuah komputer dengan HAL. Meskipun penulis fiksi-sains tersebut menolak mengakui bahwa komputer yang dinamakannya HAL merupakan penyandian dari sebuah merk komputer dalam dunia nyata, namun segera kita dapat mengasosiasikannya dengan IBM.

Percobaan pertama Blaise de Vigenère dalam modifikasi Sandi Kaisar terjadi pada tahun 1562 (Cameron, 2003), sekitar 15 abad setelah *Julius Caesar* menciptakan sandinya. Ide dasar dalam Sandi Vigenère adalah penggunaan substitusi yang berbeda untuk huruf-huruf yang berbeda dalam plaintext. Subtitusi tersebut akan menghasilkan sebuah kunci yang digunakan dengan pengulangan. Dalam Sandi Vigenère, (blok) kunci terpendek terdiri dari dua buah huruf dengan blok kunci terpanjang terdiri dari tak hingga huruf (atau sebanyak jumlah huruf dalam *plaintext*, meskipun kasus ini tidak pernah ditemukan).

Sebagai contoh, sebuah kunci dengan lima huruf akan menghasilkan barisan (5, 14, 23, 4, 18) akan menyandikan kata '*enemy*' menjadi JBBQQ (Cameron, 2003). Dalam hal ini, posisi *plaintext* (pesan asli) ditempati oleh kata *enemy* dan *ciphertext* (pesan terkirim) adalah JBBQQ (gambar 3). Barisan (5, 14, 23, 4, 18) berarti huruf pertama, keenam, kesebelas dan seterusnya untuk setiap kelipatan lima digeser 5 langkah ke kanan, huruf kedua, ketujuh, kedua belas dan seterusnya untuk setiap kelipatan lima digeser 14 langkah ke kanan, dan seterusnya. Barisan (5, 14, 23, 4, 18) akan menggeser rangkaian lima huruf $aaaaa$ menjadi *FOXES*. Dengan demikian, kunci untuk penyandian ini adalah *FOXES*.

Pesan asli (*plaintext*)	e	n	e	m	y
Kunci (*key*)	F	O	X	E	S
Pesan terkirim (*ciphertext*)	J	B	B	Q	Q

Gambar 3. Contoh Penggunaan Kunci FOXES

Secara lebih lengkap, dipaparkan pemetaan dari setiap huruf yang digunakan dalam Sandi Vigenère menggunakan kunci *FOXES* (Gambar 4). Dengan menggunakan metode pertama dalam penamaan kunci sandi, kunci tersebut

dapat dinamakan Kunci *vmdvi* yang membentuk rangkaian lambang bilangan Romawi (5+1000+500+5+1 = 1562). Angka ini menyatakan tahun saat pertama kali Blaise de Vigenère memodifikasi Sandi Kaisar.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Kunci F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
Kunci O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Kunci X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Kunci E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
Kunci S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Gambar 4. Pemetaan dengan Kunci *FOXES* atau Kunci *vmdvi*

Contoh penggunaan kunci *FOXES* dalam Sandi Vigenère sebagai berikut. Dengan menggunakan kunci *FOXES* maka pesan asli *enemy together* akan disandikan dengan JBBQQ YCDILMSO (Gambar 5). Jika pada Sandi Kaisar huruf yang sama pada pesan asli akan disandikan dengan huruf yang sama pada pesan terkirim, maka pada Sandi Vigenère kasusnya dapat sama atau berbeda. Artinya, pada Sandi Vigenère huruf yang sama pada pesan asli dapat disandikan dengan huruf yang sama pada pesan terkirim, tetapi pada umumya berbeda. Pada Gambar 4, terlihat huruf e disandikan dengan J, B, I, dan S yang seluruhnya berbeda.

Pesan asli (*plaintext*)	e	n	e	m	y	t	o	g	e	t	h	e	r
Kunci (*key*)	F	O	X	E	S	F	O	X	E	S	F	O	X
Pesan terkirim (*ciphertext*)	J	B	B	Q	Q	Y	C	D	I	L	M	S	O

Gambar 5. Contoh penggunaan Kunci *FOXES* dengan pengulangan kunci

Pemilihan kunci pada Sandi Vigenère pada umumnya berupa sebuah kata yang sederhana (misalnya FOXES, VICTORY) atau sebuah frase yang mudah diingat. Kunci yang dipilih juga dapat diubah sewaktu-waktu tergantung kesepakatan dua pihak yang berkomunikasi. Aturan ini juga digunakan dalam pemilihan kunci pada '*Lady Djamijah cipher*' yang ditemukan di Pacitan.

Sebagai pengembangan dari Sandi Kaisar, maka Sandi Vigenère juga mewarisi kelamahan yang melekat pada Sandi Kaisar. Kelemahan tersebut adalah mudahnya kunci sandi ditebak atau dipecahkan. Bagaimanapun juga, Sandi Vigenère tetap menggunakan pergeseran beberapa langkah ke kanan sehingga upaya coba-coba akan dapat dengan segera memecahkan pesan rahasia tersebut. Kelemahan kedua adalah dengan adanya pengulangan, maka huruf-huruf selanjutnya dapat mudah dipecahkan.

Sesungguhnya, kunci untuk Sandi Vigenère juga tidak dapat dikatakan mudah untuk ditemukan. Apalagi jika kunci tersebut merupakan sebuah blok yang tersusun dari semakin banyak huruf. Kunci FOXES dipandang sebagai sebuah blok dengan 5 huruf mungkin akan lebih sulit ditemukan dibandingkan blok kunci JC yang hanya terdiri dari dua huruf. Dengan demikian, penentuan panjang sebuah blok kunci pada Sandi Vigenère menjadi masalah pertama yang harus dapat dipecahkan, sebelum menemukan urutan huruf yang membentuk blok kunci tersebut.

Negeri Belanda. 1883

Ahli linguistik Belanda bernama Auguste Kerckhoffs von Nieuwenhof menerbitkan buku

La Cryptographie Militaire (Singh, 2001). Dalam buku ini termuat sebuah prinsip penyandian yang saat ini dikenal dengan namanya, *Kerckhoffs' Principle* (Singh, 2001):

> "*The security of a cryptosystem must not depend on keeping secret the crypto-algorithm. The security depend only on keeping secret the key*."

Interpretasi bebas dari prinsip ini yang selalau digunakan dalam penyandian adalah: Julius Caesar (pengirim pesan) dan Cicero (penerima pesan) harus selalu berasumsi bahwa pihak ketiga (Xerxes) mengetahui sistem pengkodean yang mereka gunakan sedemikian sehingga Xerxes akan dapat memecahkan *ciphertext* (pesan terkirim) yang diperolehnya. Ketiganya berpikir bahwa kerahasiaan pesan ini terletak pada kunci yang melindunginya..

Mengacu pada angka tahun tersebut, pastilah Kerckhoffs tahu mengenai Sandi Kaisar, Sandi Vigenère, Sandi Playfairr. Jika delapan belas tahun kemudian muncul Sandi Vigenère di Pacitan, wilayah yang menjadi jajahan Belanda, cukup besar kemungkinannya pembuat Sandi Vigenère di Pacitan pernah membaca buku Kerckhoffs, jika bukan ia sendiri pembuatnya.

Tokyo, 2 Oktober 1990

> *Finally, ... the cipher of Pacitan cracked at the first attempt, when as if by magic the computer screen showed: GDHR INNIG GELIE FDEVR OUWED JAMIJ AHGEB ORENI NACHT TIENH ....* (Remmelink, 1995).

Sebuah pusara yang saat ini masih dapat ditemukan di Pacitan menjadi bukti adanya Sandi Vigenère di Nusantara, meskipun sandi tersebut peninggalan Hindia-Belanda. Kami sendiri belum sempat untuk menyambanginya. Monumen-monumen dan pusara-pusara peninggalan VOC dan Hindia-Belanda yang masih sangat terawat di Taman Prasasti, Jakarta dan sempat disambangi, sejauh yang kami dokumentasikan tidak ada yang mengguratkan sandi. Pun demikian dengan pusara yang masih tersisa di Astana Pandu, Kota Bandung, dari dokumentasi kami tidak ada guratan sandi.

Gambar 6. Pusara yang memuat Sandi Vigenère dari Pacitan [Foto diambil dari dokumen Humas Pemkab Pacitan, Februari 2013; Sumber: https://ngrasanipacitan.wordpress.com/tag/djamijah]

Guratan Sandi Vigenère pada Pusara Djamijah (baca: Jamiyah) masih dapat disaksikan hingga hari ini di Pacitan, Jawa Timur. Kabarnya, prasasti batu nisan harus dipesan dari negeri Belanda, dan tidak dibuat di Batavia. Gambar 6 adalah pusara yang memahatkan sandi tersebut.

Petikan sandi pada pusara tersebut adalah sebagai berikut. Beberapa huruf (tanda *) tidak lagi terbaca, namun dengan berhasil di-pecahkannya sandi ini maka huruf-huruf yang tidak terbaca dapat kembali dibangkitkan (ditemukan):

Baris 1: Z * G J X F X F M F * D F W E F-

Baris 2: D X W B U J H R V W W G Z E B G-

Baris 3: Z Z. Z B A G K B M A G X B Z M Q-

Baris 4: H W G E N F W B * V W O H W X K

Baris 5: Y W O B M L * D, N N X O K W W B M

Baris 6: V X K S O T X K X W B M V X Z D-

Baris 7: E U B Q F X D D F M F D F A L M

Baris 8: V X O C W G B D F

Baris 9: H J X F W G Z E B G Z Z F V M J

Baris 10: H L R N T K R S K L M Z H B L G

Baris 11: X Q H C N J X F X I H W Y A D W G

Baris 12: E N G Z X B Z M F M Y U B S M B-

Baris 13: D D F? W B G W X I D O X O D D W

Baris 14: F R E R A Z S K Q N W M B J D X

Baris 15: F M. R T I H C N L N A M T * V X-

Baris 16: O Y A X K? Z D L B Q W X K K W

Baris 17: O B M A L E H W K K Z E T X K K

Baris 18: * * * * Z V S Z T K R A G E * *

Baris 19: * * * S W V R R R K. F Q P X Z J M

Baris 20: * * G Z L D V X K V W K A Y G *

Baris 21: * * L O R H D Z B F G H F C. V T

Baris 22: * * G F. F J R T I C W G J N W B

Baris 23: * * C X K V W Z L U W K D N D Z-

Baris 24: L S Z T K D E X K D F N T D W K

Baris 25: Q D J N D U A G A D F. M L S O X-

Baris 26: A D J S F D F L!

Dalam Sandi Vigenère dari Pacitan ini, tanda baca titik, tanda seru, tanda tanya, tanda hubung dan koma tidak disandikan. Peng-gunaan angka juga tidak ditemukan bahkan untuk mewakilinya digunakan lafal bilangan.

Untuk dapat membaca sandi rahasia tersebut, harus ditemukan kuncinya. Tulisan ini tidak mencakup kriptoanalisis yang mencoba untuk menemukan kunci dari Sandi Vigenère tersebut. Pada akhirnya, kita mendapati hal yang sungguh menarik bahwa kunci dari sandi ini adalah tahun kelahiran wanita yang dipersonifikasikan dalam sandi ini.

Willem G. J. Remmelink dengan dibantu oleh Mr. J. W. Stumpel melalui program komputer-nya, berhasil menemukan kunci untuk Sandi Vigenère pada pusara Djamijah. Kunci yang ditemukan adalah Kunci *ZSTX* (menurut versi Remmelink) yang dengan penamaan lain akan

disebut Kunci *BIHD* yang hasil penyandiannya dapat dilihat pada Gambar 7. Dalam bentuk barisan, Kunci *zstx* dapat dinyatakan dengan (25, 18, 19, 23) dan Kunci *BIHD* dinyatakan dengan (1, 8, 7, 3) yang tidak lain adalah tahun kelahiran Djamijah, wanita yang jasadnya bersemayam abadi di bawah nisan ini.

	a	b	C	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Kunci B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
Kunci I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
Kunci H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
Kunci D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Gambar 7. Pemetaan dengan Kunci *zstx* atau Kunci *BIHD*

Untuk mengingat kunci dari sandi ini, perancang sandi menggunakan angka tahun kelahiran Djamijah sebagai kuncinya. Dari angka tahun 1873 muncul barisan (1, 8, 7, 3) yang menjadi Kunci *BIHD*. Itulah kunci sandi ini. Sungguh romantis, ia yang menginisialkan dirinya dengan G.B.F.F.Q.S memilih untuk mengingat tahun kelahiran, bukan tahun kematian agar dalam dirinya, Djamijah selalu hidup dan tak mau kehilangan.

Remmelink (1995) menyebut kunci yang digunakan untuk membaca Sandi Djamijah tersebut sebagai Kunci *ZSTK*. Dengan penamaan yang berbeda, Kunci *zstx* tidak lain adalah Kunci *BIHD*. Dengan kunci ini muncul kalimat dalam bahasa Belanda. Sandi ini berhasil dipecahkan pada 2 Oktober 1990, di Tokyo.

```
a A n m y n e i n n i g g e l i-
e F d e v r o u w e d j a m i j-
a h. g e b o r e n i n a c h t t-
i E n h o n d e r d d r i e e n
z E v e n t i g, o v e r l e d e n
d E n t w a a l f d e n d e c e-
m B e r n e g e n t i e n h o n
d E r d e n e e n
o M y n d j a m i j a h m y n r
o O s v a n s a r o n h o e m o
e T i k u m y n e l i e f d e e n
h O o g a c h t i n g b e t u i-
g E n? d e h e e l e w e r e l d
i S m y d a a r t o e t e k l e
i n. z a l i k u o o i t w e d e-
r Z i e n? a l s e r e e n l e
v E n i s h i e r n a m a a l s
m O e t g y t h a n s i n h e t
p A r a d y s z y n. g y w a a r t
z O o g o e d e n w e r d z o o
m E t v u i l g e g o o i d. d a
a R o m. i k z a l d e n m o e i
l Y k e n w e g o v e r g o l g-
o T h a n e m e n e n u w e e r
t E r u g v i n d e n. t o t w e-
d E r z i e n s!
```

Terjemahan dari bahasa Belanda ke dalam bahasa Inggris telah diberikan oleh Remmelink (1995). Terjemahan bebas dalam Bahasa Indonesia kurang lebih sebagai berikut:

> *Untuk istri yang sangat kucintai Djamijah. Terlahir 1873 meninggal 12 Desember 1901. Oh Djamijah-ku, bunga mawarku (*rose of Sharon*). Bagaimana saya dapat mengungkapkan rasa cinta dan hormatku kepadamu? Seluruh dunia ini menjadi sempit bagiku. Apakah aku akan bertemu denganmu lagi? Seandainya ada kehidupan di alam baka, tentu kamu sekarang ini ada di surga. Kamu sungguh sangat baik dan begitu saja terlempari kotoran. Karena itu, saya akan menempuh jalan sulit melewati Golgotha dan menemuimu kembali. Sampai kita ketemu lagi!*

Artikel Remmelink (1995) masih menyisakan satu pertanyaan terkait dengan inisial yang dipastikan adalah suami dari Djamijah. Dengan Kunci *zstx* tentu saja dapat dipecahkan inisial tersebut. Namun, setelah dilacak pada Almanac de Gotha tidak ditemukan inisial yang bersesuaian. Inisial yang terpahat adalah G.B.F.F.Q.S dan dengan Kunci *zstx* akan menjadi H.J.M.I.R.A. Jika kita merujuk pada https://ngrasanipacitan.wordpress.com/tag/djamijah/ maka saat ini, dengan tingkat keausan dan kerusakan yang makin parah G.B.F.F.Q.S terduga baca menjadi T.B.F.F.Q.8.

Remmelink menduga orang tersebut adalah Marcus Jacobus van Erp Taalman-Kip (M.J.V.E.T.K.) yang lahir di Woerden, 16 Maret 1830. Di Jawa, Taalman-Kip tinggal di Madiun (tidak jauh dari Pacitan) dan menikahi perempuan Jawa bernama Noertya. Dikaitkan dengan artikel sebelumnya (Archipel 47), Tuan Gip yang dalam artikel tersebut adalah pendiri Monumen Pacitan dalam kisah ini, diduga Remmelink sebagai Taalman-Kip. Namun, tidak ada kunci yang dapat mengubah G.B.F.F.Q.S menjadi M.J.V.E.T.K!

Banyak pertanyaan dapat dimunculkan terkait dengan keberadaan Sandi Vigenère dari Pacitan ini. Beberapa diantaranya adalah (1) Siapakah matematikawan yang membuat sandi ini? Apakah G.B.F.F.Q.S sendiri yang menyiapkan sandinya sehingga hanya ia sendiri yang mempunyai kunci dari pesan rahasia ini? Ataukah sandi ini dipesan pada Auguste Kerckhoffs von Nieuwenhof, penulis buku *La Cryptographie Militaire*. (2) Pengetahuan matematika apa yang sudah dimiliki oleh pembuat sandi tersebut? Apakah ia mempelajarinya di Belanda atau di Hindia-Belanda? Jika di Hindia-Belanda, maka ini menjadi menarik. (3) Mengapa sandi ditulis dalam Bahasa Belanda, bukan Jawa, Melayu, atau Cina? Hal ini terkait dengan siapa yang dituju dengan sandi ini? (4) Siapakah Djamijah? Mengapa ia begitu berarti bagi lelaki yang menginisialkan dirinya dengan G.B.F.F.Q.S.? (5) Munculnya kosa kata Djamijah berarti masuknya bahasa Jawa dalam bahasa Belanda. Apakah ada makna linguistiknya? (6) Adakah metode lain untuk menemukan blok kunci ZSTX selain metode yang telah digunakan oleh Mr. J.W. Stumpel? (7) Adakah metode lain untuk memecahkan Sandi Vigenère ini yang mungkin menghasilkan kunci berbeda?

Daftar Pustaka

1. Burton, D.M. (2007). *Elementary Number Theory.* 6th ed. New York: McGraw-Hill Higher Education.

2. Cameron, P.J. (2003). *Notes on Cryptography*. Not published.

3. G.J. Remmelink, Willem (1995). *The Key to the Mysterious Epitaph of Pacitan*. Archipelago, Vol. 49, 1995, pp 17-24.

4. https://ngrasanipacitan.wordpress.com/tag/djamijah/

5. Singh, S. (2001). *The Code Break: How to Make It, Break It, Hack It, Crack It*. New York: Delacorte Press.

==========

** Agung Prabowo, M.Si., meraih gelar Sarjana dalam bidang Matematika dari ITB pada tahun 1998 dan gelar Magister dalam bidang Aktuaria pada tahun 2001. Ia kemudian menjadi dosen di Jurusan Matematika, Universitas Jenderal Soedirman, Purwokerto. Saat ini ia tercatat sebagai mahasiswa Program Doktor di FPMIPA Universitas Pendidikan Indonesia dan sedang menyusun disertasi doktornya.*