Peraturan Mengenai Kriptografi, Menjaga Privasi atau Menjaga Keamanan?

Billy Putra Taufik[1], Diana Rosida[2], dan Nugroho Muhtarif[3]

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : *if12033@students.if.itb.ac.id*[1], *speech_box@yahoo.com*[2], *teluk_kalayan@yahoo.com*[3]

Abstrak

Aplikasi kriptografi terus berkembang untuk memenuhi kebutuhan terjaminnya kerahasiaan pesan dan dokumen penting. Banyak algoritma baru yang dibuat dengan berbagai macam keunggulan agar enkripsi yang dilakukan tidak dapat diketahui. Penggunaan kriptografi dalam teknologi informasi harus didukung oleh kebijakan yang ditetapkan di setiap negara. Survey terhadap kebijakan kriptografi di seluruh dunia menghasilkan data bahwa di beberapa negara di dunia terdapat pembatasan dalam penggunaan teknologi dan produk enkripsi data untuk melindungi privasi saat online. Negara-negara tersebut mengutamakan keamanan negara dan mengenyampingkan privasi publik.

Kata kunci: kebijakan, kriptografi, pembatasan, privasi.

---

1. Pendahuluan

1.1 Komunikasi Online

Karena kebutuhan manusia semakin kompleks, seiring juga dengan kegiatan manusia yang semakin beragam, teknologi terus berkembang untuk membantu manusia. Dengan teknologi yang ada sekarang ini, manusia dapat berkomunikasi tanpa dibatasi ruang dan waktu. Komunikasi seperti ini dapat berupa percakapan melalui media telepon dan telepon seluler, percakapan melalui media internet dengan messenger, pengiriman dan penerimaan surat melalui jaringan (email), transaksi jual/beli secara online, dan sebagainya.

1.2 Kriptografi

Kriptografi adalah suatu ilmu sekaligus seni untuk menjaga kerahasiaan pesan atau secara singkat berarti cara menjaga privasi saat berkomunikasi. Untuk tujuan tersebut dilakukan enkripsi dan dekripsi terhadap pesan atau dokumen penting yang sifatnya rahasia. Enkripsi merupakan proses mengubah data menjadi bentuk yang sulit/tidak dapat dimengerti. Sedangkan dekripsi

merupakan proses pengembalian data yang telah dienkripsi menjadi bentuk yang sebenarnya dan dapat dimengerti kembali.

1.3 Kriptografi dalam Komunikasi Online

Untuk melindungi privasi pengguna komunikasi online, digunakan kriptografi. Enkripsi dilakukan terhadap suara saat bercakap-cakap melalui telepon seluler, pesan dan email yang dikirim, PIN kartu kredit/debet saat membeli barang melalui website komersial, PIN kartu ATM saat mengambil uang secara online, dan lain-lain. Dengan algoritma enkripsi yang kuat, data/pesan penting dan rahasia yang dikirim melalui jaringan tidak dapat diketahui maksudnya walaupun dapat disadap di tengah jalan.

1.4 Peraturan Mengenai Kriptografi

Pada dasarnya, peraturan tentang penggunaan kriptografi dalam teknologi informasi dibuat oleh pemerintah negara. Setiap negara berhak menentukan peraturan seperti apa yang akan diberlakukan di negaranya dengan mempertimbangkan aspek keamanan negara serta aspek privasi masyarakatnya. Peraturan ini meliputi aplikasi kriptografi yang boleh dipergunakan berdasarkan algoritma yang diimplementasikan, dan produk kriptografi apa saja yang boleh diperjualbelikan/diekspor/diimpor berdasarkan tujuan penggunaan aplikasi tersebut.

2. Ruang Lingkup

Menurut survey oleh Global Internet Liberty Campaign terhadap negara-negara di dunia, terdapat beberapa negara yang membatasi dengan ketat penggunaan produk kriptografi, seperti di Amerika, Rusia, Cina, Pakistan, dan Singapura. Di beberapa negara yang lain juga terdapat pembatasan tetapi tidak ketat seperti di Indonesia, Malaysia, Jepang, Spanyol, Afrika Selatan, dan Taiwan. Sedangkan di negara-negara lainnya teknologi kriptografi dapat digunakan dengan bebas seperti di Brazil, Denmark, Jerman, Belanda, Filipina, dan Swiss.

Negara-negara yang sangat membatasi penggunaan kriptografi biasanya ingin menghindari resiko terjadinya komunikasi rahasia untuk merencanakan gangguan keamanan seperti penyerangan dan pemberontakan. Di negara-negara seperti ini, walaupun komunikasi melalui internet maupun telepon seluler dilakukan dengan mengenkripsi data yang dipertukarkan, data-data yang telah dienkripsi tersebut tetap dapat dibaca oleh pemerintah, juga oleh *cryptanalys* karena algoritma yang diperbolehkan bukanlah *unbreakable encryption methods*.

Memang keamanan pemerintah dan negara lebih terjamin, tetapi dampak negatifnya cukup besar. Dampak negatif dari hal ini antara lain tidak ada lagi privasi bagi pribadi yang menggunakan media online untuk berkomunikasi, terganggunya kemanan dalam transaksi komersial secara online, banyaknya kemungkinan terjadi pembajakan software, dan besarnya kemungkinan terjadi pencurian/pengrusakan data-data penting oleh orang-orang yang tidak bertanggung jawab.

Pada makalah ini, kami akan membahas *trade off* yang timbul saat diberlakukannya peraturan mengenai penggunaan kriptografi yang sangat ketat serta usulan agar tidak ada pihak yang dirugikan.

3. Pembahasan

3.1 Kecepatan Pengolahan Data oleh Komputer

Mungkin tidak banyak yang sering memikirkan seberapa cepat sebuah *super computer* memproses data. Dari data yang kami peroleh, *super computer* yang biasa diperjualbelikan kecepatannya kira-kira 10.000 (sepuluh ribu) kali kecepatan komputer Pentium terbaik saat ini. Sedangkan *super computer* yang dimiliki pemerintah seperti National Security Agency (NSA) Amerika Serikat kecepatannya kira-kira 10.000 (sepuluh ribu) kali lebih cepat daripada *super computer* komersial, dengan total kecepatan 100.000.000 (seratus juta) kali lebih cepat dari *desktop computer* yang kita miliki di rumah.

Perlu juga diketahui bahwa NSA pada tahun 1983 melakukan penelitian untuk membuat sebuah komputer yang mampu mengerjakan 1.000.000.000.000.000 (satu quadrilion) multiplikasi per detik. Setelah 22 tahun berlalu, kecepatan komputer yang sudah sebegitu cepatnya pasti sudah berkali lipat lebih cepat lagi. Dengan kemampuan seperti itu, dapat dibayangkan bahwa algoritma kriptografi yang sudah rumit pun masih mungkin dapat dipecahkan dalam waktu singkat.

3.2 Peraturan Mengenai Kriptografi yang Telah Dibuat

Banyak negara yang telah menetapkan peraturan mengenai kriptografi. Di antaranya yang akan kami bahas adalah Australia, Indonesia, Singapura, dan Amerika Serikat.

Menurut Departemen Perdagangan Luar Negeri Australia, Australia mempunyai industri enkripsi komersial yang maju, dengan fokus utama pada perlindungan arus data komersial melalui modem, pengacak suara, dan telepon seluler, dan ekspor Australia untuk produk-produk kriptografi penting untuk industri keuangan. Pada Desember 1996, Australia mengamandemen hukum terhadap ekspor untuk mengizinkan pembebasan penggunaan perangkat lunak enkripsi untuk keperluan pribadi dalam kendali pengguna orang Australia. Australia tidak memberlakukan kontrol impor terhadap produk kriptografi di Australia.

Di Indonesia tidak seperti di Australia. Kedutaan Indonesia di Washington menyampaikan bahwa regulasi mengenai kriptografi untuk penggunaan domestik masih merupakan hal baru di seluruh Indonesia sehingga tidak ada pembatasan yang berarti. Badan yang bertanggung jawab dalam pembuatan peraturan mengenai ekspor dan impor produk kriptografi adalah Direktorat Jenderal Perdagangan Internasional yang berada di bawah Menteri Perdagangan dan Industri.

Berbeda dengan Indonesia, Singapura memberlakukan pembatasan terhadap produk kriptografi. Menurut Badan Pengembangan Perdagangan (TDB) Singapura, impor alat pengacak, perangkat keras pengenkripsi, perangkat lunak untuk mengubah tanda, sinyal, tulisan, suara, maupun kecerdasan untuk tujuan keamanan berada dalam pengawasan TDB di bawah peraturan regulasi impor dan ekspor tahun 1995. Sebelum barang-barang impor diperbolehkan masuk ke Singapura, harus ada surat izin tertulis dari TDB. Untuk mendapatkan surat izin tersebut, importir harus melengkapi ‘aplikasi untuk impor perangkat keras/perangkat lunak pengenkripsi’ kemudian menyerahkannya kepada perwakilan TDB. TDB akan meminta importir tersebut untuk melengkapi spesifikasi teknik dari pengenkripsi dan membuat pembenaran bagi pengguna untuk menggunakan pengenkripsi tersebut. TDB akan memberikan jawaban aplikasi. Jika diperbolehkan, importir

tersebut harus mengajukan permohonan izin kepada Badan Telekomunikasi Singapura (TAS) dan Badan Peizinan untuk menggunakan pengenkripsi tersebut (hanya untuk perangkat lunak).

Di Amerika, Regulasi Hubungan Internasional-lah yang diberi wewenang untuk mengizinkan ekspor sementara terhadap perangkat lunak pengenkripsi pada Pebruari 1996. Dengan wewenang ini, pengguna jaringan memperoleh keamanan yang cukup saat berkomunikasi online. Tetapi pada tahun yang sama, setelah melalui pemeriksaan, akhirnya wewenang untuk ekspor produk kriptografi dipindahkan kepada Departemen Perdagangan. Departemen Peradilan juga menjadi bagian dalam proses peninjauan ekspor. Dan yang menjadi penentu diberikannya izin adalah National Security Agency (NSA). Kriptografi yang menggunakan mekanisme pencarian kunci mendapatkan perlakuan yang baik dalam proses pengambilan keputusan.

Walaupun begitu, pada tanggal 3 September 1997, Kepala Federal Bureau of Investigation (FBI) mendapat perintah untuk mengawasi produk pengenkripsi Amerika Serikat yang dapat dibebaskan dari hukum dan akses pemerintah

Dukungan FBI adalah untuk mengawasi pembuatan produk pengenkripsi dan layanan jaringan untuk menggunakan pencarian kunci atau mekanisme *escrow* yang akan menghasilkan dekripsi yang cepat terhadap komunikasi maupun informasi elektronik yang terenkripsi oleh produk-produk maupun layanan-layanan tersebut dalam jaringan publik. FBI juga menentukan metode enkripsi yang sesuai dengan standar penyadapan (*eavesdropping*) pemerintah. Tidak ada teknologi baru dengan mekanisme enkripsi yang dapat dibuat, dijual, dijual kembali, diedarkan, maupun diimpor tanpa izin dari Kepala Kantor Penyelenggara Hukum di Amerika Serikat.

Di samping negara-negara di atas, juga terdapat organisasi yang menetapkan peraturan mengenai kriptografi. Organization for Economic Cooperation and Development (OECD) yang merupakan perkumpulan perusahaan-perusahaan internasional yang biasa melakukan transaksi melalui jaringan, telah cukup lama membuat peraturan sendiri agar kriptografi dapat digunakan dengan bebas (tahun 1997). Peraturan ini memang banyak mendapat dukungan dari publik, tetapi hanya beberapa negara saja yang bersedia memberlakukannya seperti Austria, Belgia, Denmark, Jerman, Yunani, Italia, Belanda, Swiss, dan Inggris.

3.3 Keadaan Negara-Negara yang Memberlakukan Pembatasan Penggunaan Kriptografi

Secara umum yang terlihat, negara-negara yang sangat membatasi penggunaan, ekspor, dan impor produk kriptografi cukup aman dari gangguan keamanan. Tetapi sebenarnya keadaan ini tidak berbeda dengan negara-negara lain yang membebaskan penggunaan, ekspor, dan impor produk kriptografi.

Yang jelas terlihat adalah banyak pihak yang merasa dirugikan dengan kebutuhan mereka akan penggunaan, ekspor, maupun impor yang dibatasi oleh negaranya. Dengan pembatasan tersebut, privasi mereka tidak terjaga. Akibatnya banyak tulisan-tulisan yang menyatakan mengenai pemerintah yang memata-matai komunikasi publik sehingga menimbulkan ketidaknyamanan.

3.4 Usulan

Banyak pihak yang berkepentingan mengeluhkan peraturan negaranya yang sangat membatasi penggunaan kriptografi. Di lain kondisi, pertukaran pesan/data sangat bebas akibat penggunaan kriptografi yang bebas pula. Kedua kondisi di atas pasti ada keunggulan dan kelemahan masing-

masing. Untuk mengurangi kelemahan-kelemahan yang ada, kami ingin memberikan beberapa usulan agar dapat dipertimbangkan yaitu:

1. Dalam transaksi jual/beli online, asalkan situs dan barang dagangannya legal, seharusnya penggunaan kriptografi dibebaskan.
2. Apabila Pemerintah sangat khawatir mengenai keamanan negara, pemerintah sebaiknya membuka pendaftaran untuk perusahaan-perusahaan dan publik yang perlu melakukan pertukaran data penting secara online. Setiap perusahaan dan orang yang mendaftar harus memberikan identitas dan deskripsi yang cukup mengenai perusahaan dan dirinya serta keperluannya dalam pertukaran data. Semua yang legal dan dapat dianggap tidak membahayakan dapat diberikan kebebasan untuk menggunakan kriptografi secara bebas dengan perjanjian.
3. Data/pesan yang dipertukarkan dengan enkripsi tetapi dianggap mencurigakan boleh saja diterjemahkan oleh pemerintah, tetapi pemerintah harus tetap menjamin kerahasiaan data/pesan tersebut.
4. Jual/beli dan ekspor/impor produk kriptografi memang sebaiknya diawasi oleh pemerintah. Sebaiknya pemerintah mengetahui identitas penjual dan pembelinya beserta tujuan penggunaan produk tersebut. Tetapi tidak perlu membatasi jenis algoritma dalam produk enkripsi yang diizinkan.

4. Kesimpulan

Kriptografi adalah suatu ilmu sekaligus seni untuk menjaga kerahasiaan pesan atau secara singkat berarti cara menjaga privasi saat berkomunikasi. Untuk tujuan tersebut dilakukan enkripsi dan dekripsi terhadap pesan atau dokumen penting yang sifatnya rahasia.

Pada dasarnya, peraturan tentang penggunaan kriptografi dalam teknologi informasi dibuat oleh pemerintah negara. Setiap negara berhak menentukan peraturan seperti apa yang akan diberlakukan di negaranya dengan mempertimbangkan aspek keamanan negara serta aspek privasi masyarakatnya.

Dengan peraturan yang ketat dalam penggunaan kriptografi, pemerintah negara bermaksud meminimalkan resiko terjadinya gangguan keamanan negara. Tetapi maksud baik tersebut menimbulkan dampak negatif seperti tidak ada lagi privasi bagi pribadi yang menggunakan media online untuk berkomunikasi, terganggunya kemanan dalam transaksi komersial secara online, banyaknya kemungkinan terjadi pembajakan software, dan besarnya kemungkinan terjadi pencurian/pengrusakan data-data penting oleh orang-orang yang tidak bertanggung jawab.

Penetapan peraturan oleh setiap negara pastinya telah dipertimbangkan dengan sungguh-sungguh oleh masing-masing pihak yang berwenang. Melalui makalah ini kami ingin memberikan beberapa pemikiran antara lain:

1. Dalam transaksi jual/beli online, asalkan situs dan barang dagangannya legal, seharusnya penggunaan kriptografi dibebaskan.
2. Apabila Pemerintah sangat khawatir mengenai keamanan negara, pemerintah sebaiknya membuka pendaftaran untuk perusahaan-perusahaan dan publik yang perlu melakukan pertukaran data penting secara online agar dibebaskan menggunakan kriptografi.

3. Data/pesan yang dipertukarkan dengan enkripsi tetapi dianggap mencurigakan boleh saja diterjemahkan oleh pemerintah, tetapi pemerintah harus tetap menjamin kerahasiaan data/pesan tersebut.
4. Jual/beli dan ekspor/impor produk kriptografi memang sebaiknya diawasi oleh pemerintah. Tetapi tidak perlu membatasi jenis algoritma dalam produk enkripsi yang diizinkan.

Daftar Pustaka

[1] EPIC, *International Cryptography Policy*, http://www.epic.com, modifikasi terakhir: 13 April 1998

[2] GILC, *Cryptography And Liberty: An International Survey Of Encryption Policy*, http://www.gilc.com, 1997

[3] R. Munir, *Diktat Kuliah IF5054 Kriptografi*, Departemen Teknik Informatika Institut Teknologi Bandung, 2005

[4] MacGregor Philips, *Top Secret Crypto Gold*, http://www.topsecretcypto.com, TAN$TAAFL Software Company, 2005

[5] B. Schneier, *December 2005 Archives*: *The Security Threat of Unchecked Presidential Power*, http://www.schneier.com, posted on December 21, 2005 at 06:50 AM