Quantum Cryptography

Albinanto, Bob, dan Hendra

Departemen Teknik Informatika
Fakultas Teknologi Industri
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail :
if11002@students.if.itb.ac.id,
if11008@students.if.itb.ac.id,
if11074@students.if.itb.ac.id

Abstrak

Satu-satunya algoritma kriptografi sempurna sehingga tidak dapat dipecahkan adalah *One-Time Pad*. Algoritma ini ditemukan pada tahun 1917 oleh Major Joseph Mauborgne. *Cipher* ini termasuk ke dalam kelompok algoritma simetri. Sistem *one-time pad* ini tidak dapat dipecahkan karena dua alasan, yaitu pertama barisan kunci acak yang ditambahkan ke pesan plainteks yang tidak acak menghasilkan cipherteks yang seluruhnya acak, dan kedua beberapa barisan kunci yang digunakan untuk mendekripsi cipherteks mungkin menghasilkan pesan-pesan plainteks yang mempunyai makna, sehingga kriptanalis tidak punya cara untuk menentukan plainteks mana yang benar. Walau begitu algoritma ini tidak digunakan secara universal dalam aplikasi kriptografi. Alasannya adalah dari segi kepraktisan, yaitu pertama karena panjang kunci harus sama dengan panjang pesan, karena itu hanya cocok untuk pesan yang pendek. Kedua, karena kunci yang dibangkitkan secara acak harus dikirimkan dari si pengirim pesan ke penerima pesan melalui jaringan. Pengiriman kunci ini sangat rentan terhadap serangan kriptanalis.

Ada sebuah solusi yang dapat mengatasi masalah tersebut, yaitu dengan teknologi *quantum mechanics* yang disebut juga *quantum cryptography*. Protokol untuk teknologi ini adalah **BB84** sesuai dengan nama pembuat dan tahun publikasinya (Bennet dan Brassard, 1984).

***Kata kunci**: kriptografi, one-time pad, quantum*

1. Pendahuluan

I can't speak without an interception.
This is private; please get off my line.
Please tell me when I can have my privacy.
– Ray & Dave Davies

Tujuan dari kriptografi adalah untuk mengantarkan informasi dengan suatu cara sedemikian sehingga informasi tersebut hanya dapat dimengerti oleh si penerima yang dimaksud oleh si pengirim informasi.

Informasi dikirim setelah melalui proses enkripsi. Informasi tersebut kini menjadi sebuah bentuk yang dinamakan cipherteks. Sesampainya di tujuan, penerima melakukan proses dekripsi agar cipherteks tersebut kembali menjadi bentuk informasi semula atau yang disebut dengan plainteks.

Pada mulanya keamanan dari kriptografi ini terletak pada algoritma enkripsi dan dekripsinya. Seiring dengan berjalannya

waktu, algoritma enkripsi dan dekripsi ini menjadi rahasia umum, sehingga kini keamanan kriptografi terletak sepenuhnya pada kunci kriptografi. Semakin panjang kunci yang dipilih maka semakin aman pula kriptografinya.

Algoritma sempurna untuk kriptografi ini adalah *one-time pad*. Sayangnya, algoritma ini tidak dapat digunakan karena sangat tidak praktis. Ada dua alasan mengapa algoritma ini tidak praktis. Pertama karena kunci yang dibangkitkan panjangnya harus sama dengan panjang plainteks. Kedua, pengiriman kunci yang panjang tersebut akan sangat susah sekali. Pengiriman tersebut sangatlah rentan terhadap berbagai serangan.

Namun teknologi quantum menjanjikan sebuah revolusi dalam keamanan kriptografi. Metode kriptografi klasik mendasarkan keamanan pada sulitnya pemecahan algoritma enkripsi dan dekripsi. Metode quantum mendasarkan keamanan pada hukum-hukum fisika, sedemikian sehingga bisa mengirimkan *one-time pad* melalui jaringan tanpa bisa diserang.

2. Dasar Quantum Cryptography

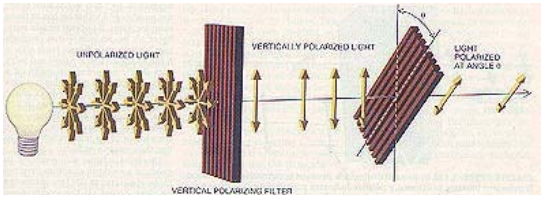
Nobody understands quantum theory.
-Richard Feynman,
Nobel prize-winning physicist

Gelombang elektromagnetik seperti gelombang cahaya dapat memperlihatkan fenomena polarisasi, yaitu arah dari vibrasi area listrik adalah tetap (konstan) atau bervariasi pada beberapa arah tertentu. Filter polarisasi adalah sebuah materi yang membolehkan cahaya dengan arah polarisasi tertentu yang dapat melewatinya. Bila sebuah cahaya dipolarisasikan secara acak, maka hanya setengahnya yang dapat melewati filter tersebut.

Berdasarkan teori quantum, gelombang cahaya dipropagasikan sebagai partikel-partikel diskrit yang disebut foton. Sebuah foton adalah partikel yang tidak bermassa, quantum dari medan elektromagnetik, yang mempunyai energi, momentum, dan momen sudut (*angular momentum*). Polarisasi dari cahaya didasarkan pada arah dari momen sudut tersebut atau arah putar (spin) dari foton.

Quantum cryptography didasarkan pada prinsip ketidakpastian Heisenberg, yang menyatakan bahwa dua buah benda berpasangan sedemikian sehingga terkait dan bila dilakukan pengukuran terhadap sifat-sifat sebuah benda maka tetap tidak akan bisa mengetahui sifat-sifat benda yang menjadi pasangan benda tersebut.

Bila seseorang mengukur polarisasi sebuah foton dengan mengamati bahwa foton tersebut melewati filter vertikal, maka dikatakan foton tersebut terpolarisasi vertikal tanpa tahu arah awalnya. Tapi bila ada orang lain yang meletakkan filter kedua sebesar Θ derajat, maka masih ada kemungkinan foton tersebut untuk melewati filter kedua, besarnya bergantung pada Θ. Semakin besar Θ maka semakin kecil kemungkinan foton akan melewatinya. Bila Θ = 90 derajat, maka foton tidak dapat melewatinya, bila Θ = 45 derajat, maka kemungkinannya adalah setengah. Dari hasil percobaan ini dapat dikatakan bahwa filter pertama menghasilkan pengukuran yang acak terhadap filter kedua.



Polarization by a filter: cahaya yang tidak berpolarisasi memasuki filter vertikal yang kemudian menyerap sebagian dari cahaya dan menyisakan sebagian yang berpolarisasi vertikal. Sebuah filter lain dengan sudut

sebesar Θ derajat kembali menyerap cahaya tadi dan membentuk polarisasi baru sebesar Θ derajat.

Bila Alice menggunakan basis filter 0/90 derajat untuk memberikan polarisasi awal terhadap sebuah foton, maka Bob akan dapat menentukan polarisasi tersebut bila ia menggunakan filter dengan basis yang sama pula. Bila Bob menggunakan filter dengan basis 45/135 derajat, maka ia tidak akan bisa menentukan informasi apapun akan polarisasi awal foton.

Karakteristik inilah yang mendasari *quantum cryptography*. Bila seorang penyadap yang bernama Eve menggunakan filter yang sama dengan Alice, maka ia dapat memperoleh polarisasi awal foton. Namun bila filter yang ia gunakan berbeda, maka ia tidak akan mendapatkan informasi apapun malahan filter tersebut akan mengakibatkan polarisasi foton berubah dan Bob akan mengetahui keberadaannya.

3. Aplikasi Quantum Cryptography

And I would send a message
To find out if she's talked,
But the post office has been stolen,
And the mailbox is locked.

- Bob Dylan

Penggunaan *quantum criptography* ini memecahkan masalah keamanan pengiriman kunci. Seorang pengguna dapat mengirimkan kunci dalam bentuk foton-foton dengan arah polarisasi yang acak secara sekuensial. Proses ini nantinya akan dibangkitkan membentuk sebuah kunci. Proses ini dinamakan distribusi kunci quantum.

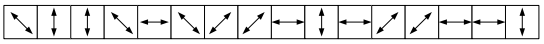
Paper pertama yang mengajukan usulan metode quantum pada aplikasi kriptografi ditulis pada tahun 1984 oleh Charles Bennet dan Gilles Brassard. Pada paper tersebut, mereka mengajukan sebuah protokol kriptografi yang aman yang bernama **BB84 *system***. Cara kerjanya adalah sebagai berikut.

Untuk membangkitkan sebuah *one-time pad*, Alice membutuhkan dua set filter polarisasi. Set pertama berisi filter vertikal dan filter horizontal. Set ini disebut ***rectilinear basis***. Set kedua adalah filter-filter yang sama namun sudutnya dirotasikan sebesar 45 derajat. Set ini disebut ***diagonal basis***. Dalam kehidupan nyata, Alice bukannya memiliki empat buah filter, melainkan sebuah kristal yang pengaturan polarisasinya dapat diatur dengan cepat. Bob juga memiliki peralatan yang sama dengan Alice.

Untuk setiap basis, Alice memberikan nilai 0 untuk sebuah arah dan 1 untuk arah yang lainnya. Misalkan vertikal adalah 0 dan horizontal adalah 1, juga sudut 45 adalah 0 dan 135 adalah 1. Informasi ini kemudian dikirimkan ke Bob.

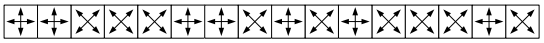
Sekarang Alice akan memilih sebuah *one-time pad* (proses ini terserah pada Alice dengan cara apa ia akan membangkitkannya). Kemudian ia kirimkan bit per bit kepada Bob. Bit-bit tersebut dikirimkan sesuai dengan nilai basis yang ia gunakan. Bit yang dikirimkan oleh sebuah foton pada satu satuan waktu dinamakan ***qubits***. Misalkan *one-time pad* Alice adalah 1001110010100110.

1	0	0	1	1	1	0	0	1	0	1	0	0	1	1	0

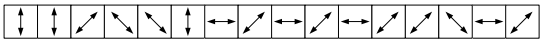


Bob tidak mengetahui basis mana yang akan digunakan, jadi ia memilih secara acak untuk setiap foton yang datang. Bila ia memilih basis yang benar maka ia akan mendapatkan bit yang benar pula. Namun bila ia salah, maka ia akan mendapatkan bit-bit yang acak.

Misalkan basis Bob :



Maka ia akan mendapatkan :



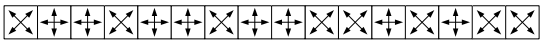
Bagaiman Bob bisa tahu mana yang benar dan mana yang salah? Bob memberitahu Alice basis mana saja yang ia gunakan untuk setiap bit dan nanti Alice akan memberitahu mana yang benar dan mana yang salah :

NO	YES	NO	YES	NO	NO	NO	YES	YES	NO	YES	YES	YES	NO	YES	NO

Dari hasil diatas, maka Alice dan Bob akan dapat membangun sebuah kunci *one-time pad* :

	0		1				0	1		1	0	0		1	

Contoh di sini hanyalah menggunakan kunci yang pendek. Bagaimana dengan Eve? Misalkan Eve ingin mengetahui pesan yang dikirimkan Alice kepada bob. Eve melakukan penyadapan dan menggunakan detektor dan transmiter miliknya. Tentu saja Eve tidak tahu basis mana yang digunakan oleh Alice. Seperti halnya Bob, ia memilih basisnya secara acak.



Ketika Bob melaporkan basis yang ia gunakan pada Alice dan Alice memberitahu Bob mana saja yang benar, Eve dapat mengetahui mana saja miliknya yang benar dan mana yang salah. Berdasarkan basis Alice, maka Eve benar untuk bit-bit 0, 1, 2, 3, 4, 6, 8, 12, dan 13. Namun berdasarkan balasan Alice terhadap Bob, hanya bit-bit 1, 3, 7, 8, 10, 11, 12, dan 14 yang merupakan baigan dari *one-time pad*. Eve menebak benar untuk bit-bit 1, 3, 8, dan 12. Untuk bit lainnya (7, 10, 11, dan 14) Eve salah. Sehingga Eve hanya dapat mempunyai bit-bit 01?1??0? sedangkan yang dimiliki Bob adalah 01011001.

X	0	X	1	X	X	X	?	1	X	?	?	0	X	?	X

Tingkat keamanan kunci ini bisa ditambahkan dengan cara melakukan transformasi. Misalkan Alice dan Bob membagi *one-time pad* mereka menjadi blok berukuran 1024 bit dan mengkuadratkannya menjadi 2048 bit angka dan menggunakan konkatenasi terhadap 2048 bit tadi sebagai *one-time pad* mereka. Dengan cara ini mustahil Eve dapat mengetahuinya. Transformasi dari *one-time pad* asli menjadi bentuk lain sehingga mereduksi kemampuan Eve untuk menyadapnya dinamakan ***privacy amplification***.

Bagi Eve, selain ia tidak berhasil menyadap Alice dan Bob, keberadaannya pun kini diketahui. Dalam proses penyadapannya, Eve harus tetap mengirimkan kembali *qubit* yang disadapnya dari Alice ke Bob dalam bentuk yang benar untuk mengelabui Bob, bahwa Bob masih berbicara dengan Alice. Dan hal ini akan sangat sulit. Masalahnya adalah Eve akan mengirimkan kembali *qubit* dari Alice menggunakan filter miliknya dan setengah dari kemungkinan tersebut adalah salah, yang kemudian akan mengakibatkan banyak *error* pada *one-time pad* milik Bob.

4. Kekurangan *Quantum Cryptography*

Metode ini sudah diujicobakan pada fiber sepanjang 60 km, dan satu-satunya kekurangannya adalah alat yang rumit dan sangat mahal.

Quantum Cryptography juga tidak memiliki perlindungan terhadap *bucket brigade attack,* atau yang lebih dikenal sebagai *man-in-the-middle attack*. Hal ini dapat terjadi, karena sulitnya mengirimkan informasi dengan menggunakan sebuah foton. Sehingga informasi pada umumnya dikirim dengan menggunakan semburan kecil cahaya koheren.

Secara teori, jika Eve dapat memisahkan sebuah foton dari semburan tersebut dan menyimpannya sampai Eve mengetahui basis yang benar, Eve dapat mengetahui kunci yang digunakan, tanpa disadari oleh Bob dan Alice.

Kelemahan lainnya dari *quantum cryptography* adalah ketidakmampuannya untuk membedakan antara *noise* dan penyadapan informasi. Hal ini memicu dua buah masalah yang potensial. Yang pertama pihak penyadap dapat menggagalkan terjadinya komunikasi dengan cara memberikan banyak error pada *one-time pad* milik Bob. Apabila Alice dan Bob mentoleransi *noise* ini untuk melakukan komunikasi, masalah kedua akan muncul, yaitu pihak penyadap (Eve) dapat melakukan penyadapan dengan lebih mudah.

5. Kesimpulan

Quantum cryptography merupakan suatu penemuan di bidang kriptografi yang dapat membantu masalah pendistribusian kunci. Kelebihan dari *quantum cryptography* terletak pada prinsip ketidakpastian Heisenberg yang menerapkan prinsip-prinsip mekanika quantum.

Seperti halnya pada algoritma kriptografi lain, *quantum cryptography* juga memiliki kelemahan. Kelemahan ini timbul selain karena ketidakmampuannya untuk membedakan penyadapan dan *noise*, juga karena sulitnya penerapan *quantum cryptography* secara sempurna dengan teknologi yang ada saat ini.

[1] Tanenbaum, Andrew, *Computer Networks*, *Fourth Edition*, Prentice Hall, New Jersey, 2003
[2] Vittorio, Salvatore, *Quantum Cryptograhy: Privacy Through Uncertainty*, http://www.csa.com, diakses tanggal 23 Desember 2004 pukul 10.12