Penerapan Kriptografi Kuantum dalam Sistem Perbankan

Juliana Amytianty K. – 13507068 [1)]

1) Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
Email : if17068@students.if.itb.ac.id

Abstrak – *Di makalah ini, dibahas mengenai penerapan kriptografi kuantum dalam sistem perbankan. Pada zaman sekarang ini, seiring dengan meningkatnya kebutuhan pengelolaan uang, terutama dalam sistem perbankan, sistem keamanan juga harus makin dapat diandalkan. Sistem perbankan biasanya menggunakan ilmu kriptografi untuk menjaga sistem keamanannya. Namun, teknik-teknik kriptografi yang biasa digunakan dalam sistem perbankan sudah dapat dipecahkan. Oleh sebab itu, diperkenalkanlah kriptografi kuantum pada sistem perbankan. Kriptografi kuantum adalah mekanisme yang menggunakan sistem kuantum untuk menjamin keamanan komunikasi. Kriptografi kuantum memiliki perbedaan dengan sistem kriptografi yang lainnya, terutama dalam pendeteksian kehadiran pihak ketiga (penyadap informasi). Pada makalah ini, akan dibahas mengenai perbedaan kriptografi kuantum dengan metode kriptografi lainnya dalam sistem keamanan perbankan. Selain itu, akan dianalisis apakah kriptografi kuantum cukup dapat diandalkan (reliable) untuk dipakai dalam sistem perbankan.*

Kata kunci: ***kriptografi, kuantum, perbankan***

1. PENDAHULUAN

Pada zaman sekarang ini, gaya hidup sebagian besar masyarakat cenderung modern, khususnya dalam mengelola dan menyimpan uang. Mengelola atau menyimpan uang di bank, bursa, dan cara pengelolaan uang modern lainnya akan semakin banyak diminati oleh masyarakat yang tingkat pendidikannya tinggi. Berdasarkan survei, sebagian besar dari pengelola uang kelas menengah di Jakarta sudah terbiasa menggunakan bank sebagai sarana untuk mengelola uangnya. Persentase terbesar pada kelas menengah baru, lebih dari 88% penduduk kelas menengah baru mempunyai simpanan uang di bank. Kelas menengah marginal sebagian besar juga mempunyai simpanan uang di bank, lebih dari 70% dari terbiasa menggunakan jasa bank untuk mengelola uangnya.

Berdasarkan data di atas, bank memiliki peranan penting dalam kehidupan masyarakat. Oleh sebab itu, keamanan menjadi hal yang sangat krusial dalam sistem perbankan. Masyarakat menginginkan sistem keamanan yang dapat dipercaya dan seaman mungkin dalam pengelolaan keuangannya. Oleh karena pentingnya sistem keamanan, studi tentang kriptografi juga amat penting dalam sistem perbankan.
Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita (menurut Bruce Schneier dalam buku *Applied Cryptography*). A. Menezes, P. van Oorschot dan S. Vanstone, dalam bukunya yaitu *Handbook of Applied Cryptography,* mengatakan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Aspek keamanan informasi yang juga merupakan tujuan mendasar dari ilmu kriptografi ini yaitu autentikasi, integritas data, kerahasiaan, dan non-repudiasi (nirpenyangkalan).

Hal pokok dalam kriptografi adalah proses enkripsi dan dekripsi pesan. Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen *plaintext* (teks biasa/normal) dan yang berisi elemen *ciphertext* (teks sandi). Enkripsi merupakan fungsi untuk menyandikan *plaintext* menjadi *ciphertext* dengan menggunakan **kunci** tertentu. Sedangkan dekripsi merupakan fungsi untuk mengembalikan *ciphertext* menjadi *plaintext* dengan menggunakan kunci yang sama pada enkripsi atau kunci yang berbeda.

Seiring berkembangnya teknologi, kriptografi berkembang sedemikan rupa sehingga tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain.

2. KRIPTOGRAFI DALAM SISTEM PERBANKAN

Teknik kriptografi yang digunakan paling umum di bank adalah kriptografi kunci simetris dan kriptografi kunci publik.

2.1. Kriptografi kunci simetris

Kriptografi kunci simetris adalah kriptografi yang baik proses enkripsi maupun dekripsi data secara keseluruhan digunakan kunci yang sama. Beberapa contoh algoritma kriptografi kunci simetris adalah :

- **DES (Data Encryption Standard)**
  DES sebenarnya merupakan standar, sedangkan algoritmanya adalah DEA (*Data Encryption Algorithm*). DES adalah kriptografi kunci simetris yang memiliki blok 64 bit dan

menggunakan kunci 56 bit. Setiap blok dienkripsi dalam 16 putaran dan setiap putaran menggunakan kunci internal berbeda. Setiap blok mengalami permutasi awal, 16 putaran *enciphering*, dan inversi permutasi awal.

Namun, DES untuk saat ini sudah dianggap tidak aman lagi. Penyebab utamanya adalah ukuran kuncinya yang dianggap sangat pendek. Di bulan Januari 1999, distributed.net dan *Electronic Frontier Foundation* bekerja sama untuk memecahkan kunci DES secara publik dalam waktu 22 jam 15 menit. Terdapat juga beberapa hasil analitis yang menunjukkan kelemahan teoretis di dalam *cipher* , walaupun hasil- hasil tersebut susah untuk dilaksanakan dalam prakteknya.

- **3DES (*Triple DES*)**
  Triple DES adalah algoritma yang mengaplikasikan DES sebanyak 3 kali dalam tiap blok.

- **AES (Advanced Encryption Standard)**
  AES memiliki 3 kategori, yaitu AES-128, AES-192 and AES-256, yang diambil dari algoritma asli yang bernama **Rijndael**. Prinsip dasar AES diketahui sebagai jaringan permutasi subtitusi. AES tidak menggunakan jaringan Feistel seperti DES. AES memiliki ukuran blok yang tetap yaitu 128 bit dan ukuran kunci 128, 192, atau 256 bit, padahal Rijndael dapat menggunakan ukuran blok dan kunci kelipatan 32 bit, dengan maksimum 128 bit. Ukuran blok memiliki ukuran maksimum 256 bit, namun ukuran kunci secara teori tidak memiliki nilai maksimum.

2.2. Kriptografi kunci asimetris (kunci publik)

Kriptografi kunci publik menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Skema ini disebut juga sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (*public-key*) atau dapat diketahui siapa saja, tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang memiliki kunci rahasia untuk mendekripsinya, disebut *private-key*. Biasanya kriptografi kunci publik tidak digunakan untuk mengenkripsi pesan karena relatif lambat, karena banyak operasi perpangkatan yang berulang-ulang, apalagi jika ukuran pesannya besar. Kriptografi kunci publik biasanya digunakan untuk mengenkripsi kunci simetri pada kriptografi kunci simetris, karena panjang kunci simetri relatif pendek. Bisa dikatakan, kriptografi kunci publik melengkapi atau menutupi kelemahan kriptografi kunci simetris. Contoh algoritma kunci publik adalah:

- **RSA (Rivert-Shamir-Adelman)**
  RSA merupakan algoritma pertama yang cocok untuk *digital signature* seperti halnya enkripsi. RSA merupakan salah satu yang paling maju dalam bidang kriptografi *public key*. RSA masih digunakan secara luas dalam protokol *electronic commerce*, dan dipercaya dalam mengamnkan dengan menggunakan kunci yang cukup panjang. RSA dapat juga digunakan untuk mengesahkan sebuah pesan, dengan membangkitkan suatu *hash value* RSA memiliki kecepatan yang lebih lambat dibandingkan dengan DES dan algoritma simetrik lainnya. Kerumitan dalam algoritma RSA adalah memfaktorkan bilangan besar ke bilangan prima.

- **Diffie-Hellman**
  Ide kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) muncul pada tahun 1976.
  Makalah pertama perihal kriptografi kunci-publik ditulis oleh Diffie-Hellman (ilmuwan dari Stanford University) di IEEE.
  Diffie-Hellman adalah protokol kriptografi yang membolehkan dua pihak yang tidak memiliki persetujuan satu dengan yang lain dapat membangun kunci rahasia melalui saluran komunikasi yang tidak aman.
  Algoritma ini dapat digunakan untuk mempertukarkan kunci simetri.

2.3. Teknik kriptografi dalam sistem perbankan

Sebenarnya di dalam sistem perbankan atau yang berkaitan dengan keuangan, ada yang disebut dengan kriptografi finansial.

Kriptografi finansial melingkupi mekanisme dan algoritma untuk perlindungan transaksi keuangan, dalam membangun bentuk baru dari keuangan. Algoritma kriptografi utama yang digunakan untuk perlindungan transfer dana adalah DES. Kriptografi finansial berbeda dengan kriptografi tradisional yang dalam sejarahnya digunakan hampir semua untuk kepentingan militer dan diplomatis.

Sebagai bagian dari model bisnis, kriptografi finansial mengikuti aturan kriptografi dan hanya ide-ide sederhana yang diambil. Sistem akun keuangan yang dilindungi oleh SSL (*Secure Socket Layer*) seperti PayPal, e-gold, dan GoldMoney secara relatif sukses. Namun mekanisme yang lebih inovatif seperti *blinded token money* tidak terlalu sukses.

Dalam dunia perbankan, beberapa algoritma yang dipakai misalnya adalah RSA dan DES. RSA merupakan algoritma kriptografi yang dianggap aman, karena RSA memiliki pemfaktoran bilangan prima yang sangat besar. Sedangkan DES merupakan algoritma yang menjadi pilihan untuk menjaga keamanan data. Misalnya digunakan dalam kartu chip yang dimiliki oleh para nasabah bank.

Sebagai contoh, sebagian besar bank pasti

menyediakan ATM (*Automated Teller Machine*). ATM adalah perangkat telekomunikasi yang terkomputerisasi yang menyediakan sisi *client* dari suatu institusi finansial dengan akses ke transaksi finansial di tempat umum tanpa berhubungan dengan kasir, pegawai, atau *teller.* ATM digunakan nasabah bank untuk melakukan transaksi perbankan. Utamanya, kegunaan ATM adalah untuk menarik uang secara tunai. Namun saat ini ATM juuga digunakan untuk transfer uang, mengecek saldo, membayar tagihan kartu ponsel, membeli tiket kereta api, dan sebagainya. Sebagian besar ATM terhubung dengan jaringan interbank, yang membuat orang dapat melakukan penarikan tunai dan menyetor uang melalui mesin yang tidak dimiliki bank yang memiliki akun orang tersebut atau di negara di mana akun orang tersebut dipegang. Oleh sebab itu, faktor keamanan di dalam ATM sangat krusial dan harus diperhatikan dengan baik.

Gambar 1: Mesin ATM

Terdapat beberapa faktor keamanan dalam ATM, salah satunya adalah faktor integritas dan kerahasiaan transaksi. Keamanan dalam tansaksi ATM kebanyakan bergantung pada integritas dari kriptoprosesor yang aman. ATM sering menggunakan komponen yang tidak bisa disebut sebagai sistem yang aman. Enkripsi dari informasi pribadi, yang terdapat dalam hukum di banyak yuridiksi, digunakan untuk mencegah penipuan. Data sensitif di transaksi ATM biasanya dienkripsi dengan DES, namun sekarang prosesor transaksi memerlukan penggunaan Triple DES. Teknik *Remote Key Loading* digunakan untuk memastikan kerahasiaan inisialisasi kunci enkripsi di ATM. MAC (*Message Authentication Code*) atau *Partial MAC* juga bisa digunakan untuk memastikan pesan tidak dirusak pada waktu berada antara ATM dan jaringan finansial.

Selain ATM, fitur perbankan yang lain adalah *anonymous internet banking*. Nama ini diberikan dengan tujuan penggunaan kriptografi finansial yang kuat untuk membentuk kerahasiaan *electonic bank. Anonymous internet banking* menggunakan kriptografi kunci publik dan algoritma *blind signature*. Algoritma kunci publik yang digunakan adalah RSA. Misalkan kita memiliki Alice dan Bob serta seorang banker. Banker membuat sebuah kunci publik RSA, kemudian bank juga akan membangkitkan kunci publik dan kunci privatnya.

Sayangnya, algoritma-algoritma kriptografi yang sudah disebutkan di atas sudah dapat dipecahkan. Sehingga, teknik kriptografi tersebut tidak benar-benar menjamin data yang dienkripsi dapat sampai ke penerima tanpa gangguan yang bisa diatasi.

3. ONE TIME PAD (OTP)

Ada satu algoritma kriptografi yang saat ini belum dapat dipecahkan, yaitu *one time pad.* Algoritma ini tidak dapat dipecahkan kecuali oleh seseorang yang memiliki kuncinya. *One time pad* adalah algoritma kriptografi kunci simetri.

One time pad adalah satu-satunya sistem enkripsi yang aman tanpa syarat sampai sekarang ini. OTP mungkin aman tanpa syarat, hal ini berarti kita tidak dapat memecahkannya dengan berbagai waktu komputasi. Agak mustahil untuk memecahkan OTP secara matematika.

Untuk menggunakan OTP, kita membutuhkan 2 duplikat dari *pad* (kertas bloknot) yang merupakan data acak yang sama panjangnya dengan pesan yang akan kita enkripsi. Maksud acak di sini adalah benar-benar acak (*truly random,* bukan *pseudo random*).

OTP digunakan berpasangan. Satu duplikat *pad* disimpan oleh pengguna, dan *pad* harus ditukarkan melalui saluran yang aman (misalnya: bertemu langsung). *Pad* digunakan dengan meng-XOR-kan semua bit dalam *pad* ke bit pesan yang asli. Sekali *pad* digunakan, *pad* tersebut langsung dihancurkan dan pesan yang terenkripsi pun dikirim. Di sisi penerima, pesan terenkripsi di-XOR dengan duplikat *pad* dan didapatkanlah pesan aslinya.

Gambar 2: *Russian OTP*

Mengapa OTP tidak dapat dipecahkan? Karena kunci yang dipilih (*pad*) benar-benar acak, yang memiliki sedikit sekali peluang untuk terpilih kembali, bahkan hampir tidak ada peluang. Selain itu, sekali suatu kunci dipilih dan dipakai, kunci tersebut langsung dihancurkan tanpa jejak. Oleh sebab itu, pesan sandi yang dihasilkan pun benar-benar acak. Alasan lainnya yaitu karena beberapa barisan kunci yang digunakan untuk mendekripsi bisa menghasilkan lebih dari satu *plaintext* yang memiliki makna, sehingga penyadap akan kesulitan dalam menentukan kunci yang benar. Selain itu, panjang kuci juga sama dengan panjang pesan yang akan dienkripsi.

Memang OTP adalah sistem kriptografi yang mengagumkan, namun tidak banyak yang menggunakannya. Hal ini terjadi karena jika kita menggunakan OTP, kunci yang kita punyai harus sepanjang pesan aslinya, sehingga OTP cocok untuk pesan yang berukuran kecil, sehingga semakin besar pesannya, kuncinya pun akan semakin besar. Hal ini menimbulkan permasalahan dalam penyimpanan dan pendistribusian kunci. Selain itu, karena kuncinya dibangkitkan dengan benar-benar acak, hampir mustahil pengirim dan penerima membangkitkan kunci yang sama pada saat yang dibutuhkan, sehingga kunci harus dikirim ke pihak lain. Jadi saluran komunikasi harus benar- benar terjamin untuk pendistribusian kunci. OTP hanya dapat digunakan jika tersedia saluran komunikasi kedua yang cukup aman untuk mengirimkan kunci. Saluran kedua ini umumnya lambat dan mahal. Misalnya pada perang dingin antara AS dan Uni Sovyet dulu, kunci dikirim melalui jasa kurir yang aman. Saluran kedua yang aman tersebut lambat dan mahal. Oleh karena alasan-alasan inilah OTP tidak terlalu banyak digunakan.

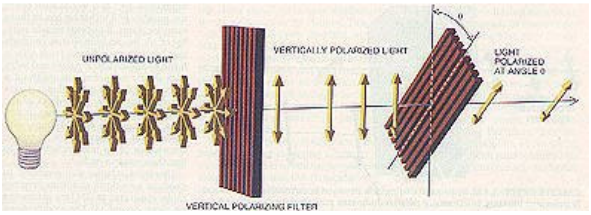
Namun, terdapat teknik untuk mengatasi masalah pendistribusian kunci dalam OTP di jaringan, yaitu dengan **teknik mekanika kuantum**.

4. KRIPTOGRAFI KUANTUM

Sistem kriptografi kuantum adalah sistem distribusi kunci yang berusaha untuk menghubungkan keamanan sistem dalam kebenaran prinsip mekanisme kuantum yang tidak pasti. Properti yang penting dan unik dari kriptografi kuantum adalah **kemampuan dua pengguna yang berkomunikasi untuk mendeteksi kehadiran pihak ketiga yang mencoba mengetahui kuncinya.** Komunikasi kuantum menggunakan *encoding information* di *quantum state*, atau *qubit* (quantum bit / satuan informasi kuantum), yang merupakan lawan dari komunikasi klasik yang menggunakan bit. Biasanya, yang digunakan untuk *quantum state* ini adalah foton. Kriptografi kuantum memanfaatkan properti tertentu dari kuantum ini untuk meyakinkan keamanannya. Kriptografi kuantum melengkapi OTP dalam mengatasi masalah pendistribusian kunci.

4.1. Dasar Teori Kriptografi Kuantum

Dasar dari kriptografi kuantum adalah fakta bahwa cahaya datang dalam paket kecil bernama **foton**. Foton memiliki sifat yang khas. Kemudian, cahaya dapat dipolarisasi dengan melewati filter polarisasi. Fakta ini terkenal di kalangan pemakai kacamata hitam anti-matahari dan fotografer. Jika cahaya melewati filter polarisasi, semua foton yang muncul melalui filter akan terpolarisasi dalam arah filter (misalkan filter vertikal). Jika cahaya sekarang melewati filter polarisasi kedua, intensitas cahaya yang keluar dari filter polarisasi kedua berbanding lurus dengan kuadrat dari kosinus sudut µ. Sudut µ adalah sudut antara cahaya yang datang dengan arah filter polarisasi. Jika sudut µ yang terbentuk bernilai 90^0, yang artinya cahaya yang datang berarah tegak lurus dengan arah filter polarisasi, tidak ada foton yang keluar. Orientasi absolut dari dua filter ini tidaklah penting, yang penting adalah sudut µ yang terbentuk dari cahaya yang datang dengan arah filter polarisasi. Jika filter terletak 45^0 dari polarisasi foton, foton yang terlewat adalah sebanyak 50%.



Gambar 3 : Polarisasi dengan filter

4.2. Mekanisme Kriptografi Kuantum

Mekanisme kriptografi kuantum ini masih bersifat eksperimental, tetapi percobaan awal menjanjikan. Jika bisa disempurnakan dan menjadi lebih efisien, semua teknik kriptografi akan diselesaikan menggunakan *One Time Pad,* karena teknik ini aman. Di bawah, akan dibahas sebuah protokol yang disebut BB84 (Bennet and Brassard, 1984) yang mengimplementasikan kriptografi kuantum. Dalam hal ini implementasi kriptografi kuantum adalah QKD (Quantum Key Distribution).

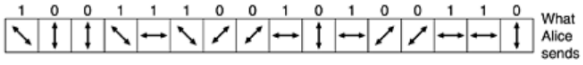
Seorang pengguna, sebut saja Alice, mau membangun teknik OTP dengan pengguna kedua, yang bernama Bob. Alice dan Bob adalah karakter utama dalam cerita ini. Misalkan Alice ingin bekerja sama dalam hal bisnis dengan Bob yang adalah banker.

Jika Alice dan Bob dapat membangun OTP, mereka harus memiliki saluran komunikasi yang aman. Pertanyaannya adalah: Bagaimana mereka membangunnya tanpa bertukar DVD sebelumnya? Dapat diasumsikan bahwa Alice dan Bob berada pada ujung-ujung dari fiber optik di mana pulsa cahaya dapat dikirim dan diterima melalui fiber optik tersebut. Akan tetapi, seorang penyadap, anggap saja namanya Trudy, dapat memotong fiber tersebut dan menyambungkannya pada alat penyadap. Trudy bisa saja membaca semua bit dari kedua arah (dari Alice

dan Bob). Dia bisa juga mengirim pesan yang palsu ke kedua arah. Situasi ini tampak tidak dapat diharapkan untuk Alice dan Bob, tetapi kriptografi kuantum dapat membuka jalan keluar untuk masalah ini.

Untuk membangkitkan OTP, Alice membutuhkan dua kumpulan filter polarisasi. Kumpulan pertama berisi filter vertikal dan filter horisontal. Pilihan ini disebut **basis rectilinear**. Sebuah basis adalah sistem koordinat. Kumpulan kedua mirip dengan kumpulan pertama, hanya saja dirotasi 45^0. Pilihan ini disebut **basis diagonal**. Jadi, Alice memiliki dua basis, yang bisa dimasukkan cahaya kapan pun. Dalam kenyataannya, Alice tidak memiliki empat filter terpisah, tetapi sebuah kristal yang polarisasinya dapat dihubungkan secara elektrik dengan 4 arah pada kecepatan besar. Bob memiliki peralatan yang sama dengan Alice. Fakta bahwa Alice dan Bob masing-masing memiliki dua basis merupakan hal penting dalam kriptografi kuantum.

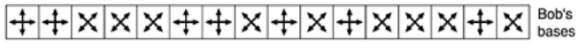
Untuk setiap basis, Alice memberikan satu arah sebagai 0 dan yang lainnya 1. Dalam gambar di bawah, misalnya Alice memilih arah vertikal menjadi 0 dan arah horisontal menjadi 1. Secara terpisah, Alice juga memilih arah kiri-bawah-kanan-atas sebagai 0 dan kiri-atas-kanan-bawah sebagai 1. Dia pun mengirim pilihan ini ke Bob sebagai *plaintext.*



Gambar 4: Yang dikirim Alice

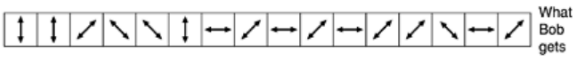
Sekarang Alice melakukan teknik OTP. Dia melakukan transfer bit per bit kepada Bob, dengan memilih salah satu dari dua basis secara acak tiap bit. Untuk mengirimkan bit, penembak foton Alice memancarkan satu foton yang terpolarisasi secara tepat ke basis yang dia gunakan untuk bit tersebut. Sebagai contoh, dia mungkin memilih basis diagonal, rectilinear, rectilinear, diagonal, dan seterusnya. Untuk mengirim OTP 1001110010100110 dengan basis ini, dia akan mengirim foton seperti pada Gambar 3. Polarisasi untuk menggunakan setiap bit diidentifikasi dengan kunci OTP yang diberikan dan urutan basisnya. Bit-bit mengirim satu foton pada satuan waktu yang disebut qubit (*quantum bit*).

Bob tidak mengetahui basis mana yang digunakan, jadi dia mengambil satu basis acak untuk setiap foton yang sampai dan menggunakannya, seperti yang ditunjukkan di Gambar 4.



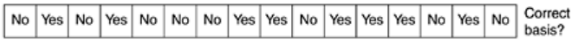
Gambar 5: Basis Bob

Jika dia mengambil basis yang benar, dia akan mendapat bit yang benar. Jika dia mengambil basis yang salah, dia mendapat bit acak karena jika sebuah foton melalui filter yang terpolarisasi 45^0 dari polarisasinya, secara acak foton akan melompat ke polarisasi filter atau ke polarisasi tegak lurus dengan filter dengan kemungkinan yang sama. Sifat foton inilah yang merupakan hal dasar dalam mekanika kuantum. Oleh sebab itu, beberapa bit benar dan nenerapa bit salah, tetapi Bob tidak mengetahui mana yang benar. Hasil yang dimiliki Bob ditunjukkan di Gambar 5.

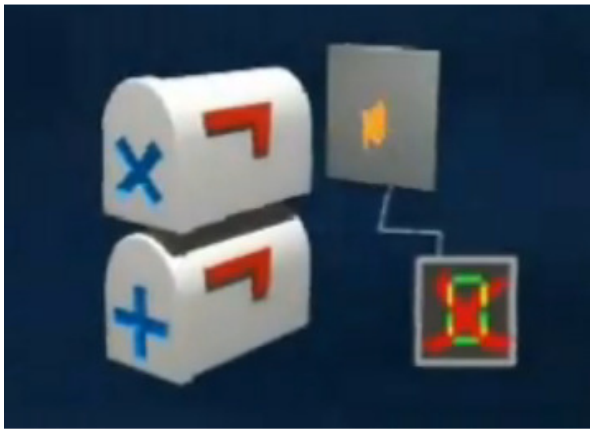


Gambar 6: Hasil yang diperoleh Bob

Bagaiamana Bob mengtahui basis mana yang salah dan basis mana yang benar? Dia akan memberitahu Alice basis apa yang digunakannya untuk setiap bit di *plaintext* dan Alice akan memberitahu Bob mana yang benar dan mana yang salah, seperti yang ditunjukkan pada Gambar 6.

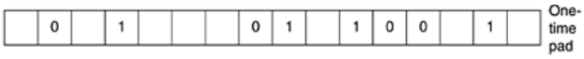


Gambar 7: Konfirmasi basis oleh Alice



Gambar 8: Ilustrasi konfirmasi basis

Dari informasi ini, keduanya dapat membangun string dari bit yang benar, seperti yang ditunjukkan pada Gambar 7.

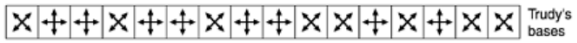


Gambar 9: String dari bit yang benar

String ini merupakan sebagian dari string seluruhnya yang dikirim Alice. Namun karena dua pihak mengetahui ini, mereka bisa menggunakannya sebagai OTP. Yang harus Alice lakukan adalah mengirimkan string bit lebih dari dua kali panjang yang diinginkan. Lalu Alice dan Bob memiliki OTP dengan panjang yang diinginkan. Masalah selesai.

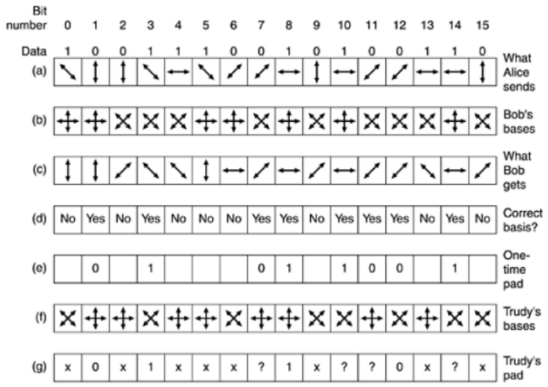
Namun, kemudian Trudy penasaran tentang apa yang Alice katakan dan memotong fiber dan memasukkan

detektor dan *transmitter*-nya sendiri. Sayangnya, Trudy tidak mengetahui basis apa yang digunakan untuk setiap foton. Yang terbaik yang dapat dia lakukan adalah memilih basis acak untuk setiap foton, sama seperti yang Bob lakukan. Sebagai contoh, pilihan Trudy ditunjukkan pada Gambar 8.



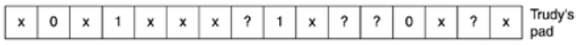
Gambar 10: Basis pilihan Trudy

Ketika kemudian Bob melaporkan basis apa yang dia pilih dan Alice mengatakan pada Bob mana yang benar dan yang salah, Trudy akan mengetahui ketika dia benar atau salah.



Gambar 11: Rangkaian cerita Alice, Bob, dan Trudy

Dari Gambar 9, Trudy benar untuk bit 0, 1, 2, 3, 4, 6, 8, 12, dan 13, tetapi Trudy mengetahui dari balasan Alice di Gambar 6 bahwa hanya bit 1, 3, 7, 8, 10, 11, 12, dan 14 yang merupakan bagian dari OTP. Untuk 4 bit yang cocok ini (1, 3, 8, dan 12), Trudy menebak bahwa itu yang benar dan mengambil bit yang benar tersebut. Untuk 4 bit lain yang tidak cocok, dia beranggapan itu salah dan tidak mengetahui bit dikirim. Oleh sebab itu, Bob mengetahui OTP dimulai dengan 01011001, dari Gambar 7 tetapi yang Trudy punya adalah 01?1??0? dari Gambar 10.



Gambar 12: *Pad* yang dimiliki Trudy

Tentu saja, Alice dan Bob menyadari Trudy mungkin telah mengambil elemen dari OTP mereka, jadi mereka akan mengurangi informasi yang dimiliki Trudy. Mereka bisa melakukannya dengan membuat perubahan dari OTP mereka. Sebagai contoh, mereka dapat membagi OTP ke blok berisi 1024 bit dan menguadratkan setiap satu blok ke bentuk 2048 bit dan menggunakan konkatenasi 2048 bit ini sebagai OTP. Dengan pengetahuan Trudy yang sebagian saja tentang string bit yang dikirim, Trudy tidak memiliki cara untuk membangkitkan kuadratnya dan jadinya tidak memiliki apa-apa. Perubahan dari OTP asli ke OTP yang baru yang membuat Trudy berkurang pengetahuannya disebut **amplifikasi privasi.** Dalam prakteknya, perubahan kompleks di mana setiap bit output tergantung pada setiap bit input digunakan sebagai pengganti penguadratan.

Sekarang, Trudy tidak hanya tidak mengetahui OTP atau kuncinya, tetapi juga keberadaannya sudah disadari. Setelah ini semua, dia harus menyampaikan setiap bit yang diterima kepada Bob untuk membuat Bob berpikir bahwa ia berbicara pada Alice. Masalahnya adalah, yang terbaik yang bisa dia lakukan adalah mengirimkan qubit yang diterimanya, menggunakan polarisasinya sendiri, dan separuh waktu dia akan salah, menyebabkan banyak kesalahan di OTP milik Bob.

Ketika Alice akhirnya mulai mengirim data, dia melakukan *encoding* dengan kode *heavy forward-error-correcting*. Dari sudut pandang Bob, kesalahan 1 bit di OTP sama dengan 1 bit kesalahan di transmisi. Mungkin dalam prosesnya, Bob akan mendapat bit yang salah. Jika ada cukup koreksi *forward-error,* Bob dapat mengembalikan pesan asli walaupun ada yang salah salah, namun dia dapat dengan mudah menghitung berapa kesalahan yang dikoreksi. Jika jumlah ini lebih dari kesalahan di peralatan, Bob tahu ada penyadap (Trudy) dan akan bertindak untuk mengatasi penyadap ini. Jika Trudy memiliki cara untuk menggandakan foton sehingga dia memiliki satu foton untuk inspeksi dan lainnya untuk dikirim ke Bob, dia bisa menghindari deteksi penyadap, tetapi sekarang, tidak ada cara yang diketahui untuk menggandakan sebuah foton dengan sempurna. Namun walaupun Trudy dapat menggandakan foton, nilai kriptografi kuantum untuk membangun OTP tidak berkurang.

Walaupun kriptografi kuantum telah diimplementasikan untuk beroperasi lebih dari fiber 60 km, peralatannya kompleks dan mahal. Namun walaupun begitu, ide ini masih menjanjikan.

5. KRIPTOGRAFI KUANTUM DALAM SISTEM PERBANKAN

Dalam sistem perbankan, kriptografi kuantum dapat diandalkan untuk menjaga keamanan dari produk dan proses yang ada di dalam bank.

5.1. Transfer bank berdasarkan *entangled photon*

Salah satu contoh bank atau institusi finansial yang sudah menerapkan kriptografi kuantum adalah Bank Austria Creditanstalt. Bank Austria Creditanstalt di Vienna, Austria, sekarang sudah menjadi bank pertama yang melakukan transfer dengan kriptografi kuantum. Kunci untuk mengenkripsi informasi diproduksi dengan pasangan *entangled photon*. Fisikawan Austria, Erwin Schrödinger memperkenalkan *entanglement* sebagai karakteristik

esensial dari fisika kuantum.

Mekanismenya adalah sebagai berikut. Di stasiun pengirim di kantor cabang bank ini, sebuah laser memproduksi dua pasang *entangled photon* dalam kristal. Salah satu dari foton dikirim melalui saluran data fiber kaca ke City Hall, yang lainnya tetap berada di bank. Kedua foton ini kemudian mengukur sifat partikelnya. Hasil yang terukur kemudian diubah ke 0 atau 1 yang merupakan kunci kriptografi. Urutan nomor 0 dan 1 bersifat acak. String yang identik dari nomor yang acak ini digunakan sebagai kunci untuk mengenkripsi (*encoding*) informasi dan diproduksi baik di bank maupun di City Hall. Pesan asli dihubungkan dengan kunci bit per bit dan kemudian ditransfer via saluran data fiber kaca.

Penyadap dapat dideteksi selama produksi kunci, bahkan sebelum transfer pesan yang terenkripsi dilakukan. Intervensi ke transfer foton mengubah urutan nomor string di stasiun pengukuran. Dengan membandingkan potongan-potongan kunci, usaha penyadap bisa terlihat.

Transfer bank menghabiskan fiber optik sepanjang lebih dari 1,45 km, yang dipasang di jaringan bawah tanah Vienna. Para peneliti menggunakan dioda laser violet sebagai sumber pompa (berada di lokasi Alice) untuk membuat 8200 pasang *entangled photon* per detik, dengan panjang gelombang 810 nm.

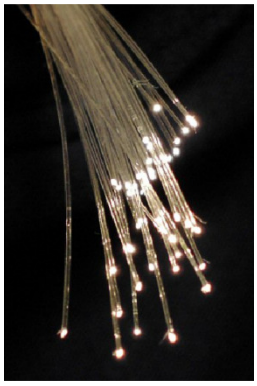
5.2. Penerapan kriptografi kuantum dalam ATM

Contoh yang disebutkan di atas adalah bank yang melakukan transfer dengan kriptografi kuantum. Pada contoh di atas, pengirim dan penerima merupakan objek tunggal, atau dapat dikatakan relasinya adalah satu-ke-satu (*one-to-one*). Di bawah ini akan dijelaskan mengenai ide penerapan kriptografi kuantum dalam produk perbankan lainnya, yaitu ATM. Sebuah bank dalam satu kota pasti memiliki minimal satu ATM. Jika ingin dibangun implementasi kriptografi kuantum untuk sistem ATM, dapat dikatakan relasi yang ada adalah satu-ke-banyak (*one-to-many*). Pada zaman sekarang, ATM dari berbagai macam bank tersedia hampir di semua tempat-tempat umum. ATM relatif tidak sulit untuk ditemukan.

Proses transaksi lewat ATM memerlukan kartu magnetik, yang disebut juga kartu ATM yang terbuat dari plastik dan berisi informasi tentang PIN (*Personal Identification Number*) yang berhubungan dengan kartu tersebut. PIN terdiri dari 4 atau 6 angka yang harus dijaga kerahasiannya oleh pemilik kartu, karena orang lain yang mengetahui PIN dapat menggunakan kartu ATM untuk tujuan yang tidak benar. PIN digunakan untuk memverifikasi kartu yang dimasukkan oleh nasabah di ATM. Proses verifikasi dilakukan di komputer pusat bank, oleh karena itu harus ada komunikasi dua arah antara ATM dan komputer pusat. ATM mengirim PIN dan informasi tambahan pada kartu ke komputer pusat. Kemudian komputer pusat melakukan verifikasi dengan cara membandingkan PIN yang dimasukkan oleh nasabah dengan PIN yang disimpan di dalam basis data komputer pusat, lalu mengirimkan pesan tanggapan ke ATM yang menyatakan apakah transaksi dapat dilanjutkan atau ditolak.

Selama proses transmisi dari ATM ke komputer pusat, PIN harus dilindungi dari penyadapan oleh orang yang tidak bertanggungjawab. Bentuk perlindungan yang dilakukan selama transmisi adalah kriptografi, yaitu dengan mengenkripsi PIN. PIN yang disimpan di basis data bank juga dienkripsi. Algoritma enkripsi yang digunakan ATM saat ini adalah DES dengan mode ECB.

Penerapan kriptografi kuantum adalah pada saat PIN dikirim ke komputer pusat di bank. Algoritma yang akan digunakan adalah *one time pad.* Algoritma ini dipakai selain untuk mendukung kriptografi kuantum, panjang data yang akan dienkripsi juga tidak terlalu panjang, yaitu sepanjang PIN.



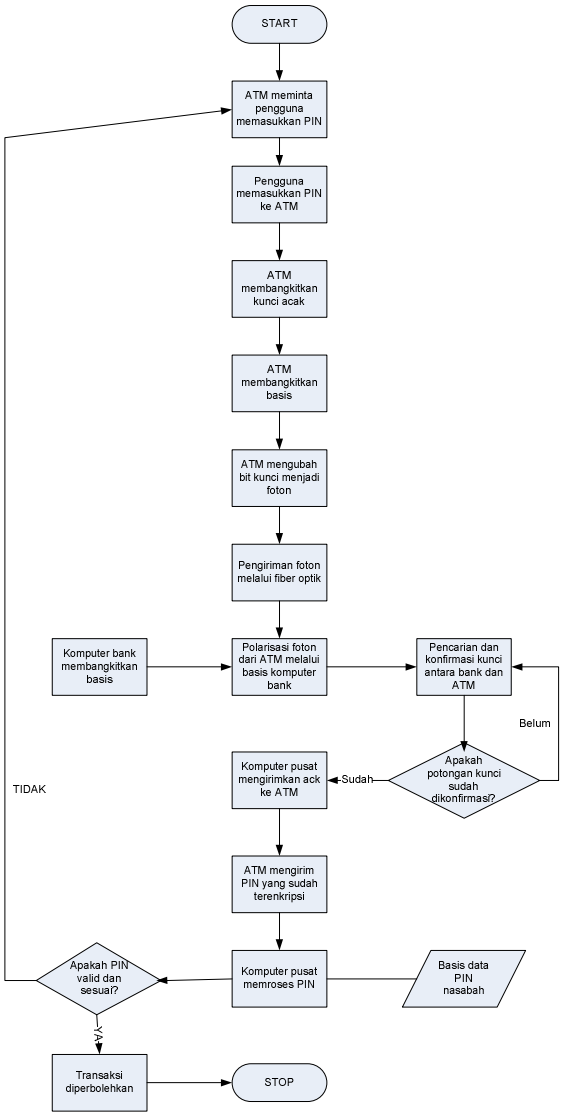
Gambar 13: Fiber optik

Dalam implementasinya, sebuah bank memiliki koneksi fiber optik ke semua ATM-nya. Dalam hal ini, dibatasi hanya untuk satu kota saja dulu. Dari masing- masing ATM, dipasang program yang digunakan untuk membangkitkan kunci acak sesuai panjang PIN orang yang bersangkutan dan basis (rectilinear atau diagonal) per bit. ATM juga dapat membangkitkan foton-foton yang merepresentasikan kunci yang dibangkitkan sesuai dengan program yang telah dibuat (representasi foton yang menunjukkan 0 atau 1 bisa sama dengan penjelasan mekanisme kriptografi kuantum di atas). Setelah itu foton dikirim dengan metode kriptografi kuantum seperti yang telah dijelaskan di atas.

Di komputer pusat, foton yang diterima kemudian diterjemahkan ke bit-bit dengan basis rectilinear atau diagonal yang dibangkitkan oleh program komputer pusat. Setelah kunci diproses sampai diketahui oleh komputer pusat, komputer pusat akan mengirimkan semacam *acknowledge* ke ATM tersebut yang menyatakan bahwa kunci sudah diketahui. Setelah itu,

baru PIN yang sudah terenkripsi dikirimkan ke komputer pusat di bank. Setelah itu PIN didekripsi dengan menggunakan potongan kunci dan dicocokkan dengan basis data komputer pusat.

Jika ada penyadap, seperti yang sudah dijelaskan di atas, keberadaannya akan terdeteksi, dan komputer pusat akan melakukan tindakan pencegahan dan penanggulangan aksi penyadap.



Gambar 14: Diagram alir proses pencocokan PIN di ATM dengan kriptografi kuantum

Masalah dari implementasi ini adalah penanganan yang harus dilakukan apabila ada dua atau lebih ATM yang mau mengirimkan foton pada saat yang bersamaan. Bisa saja di komputer pusat, dibuat penanganan *multitasking* atau dibuat sistem terdistribusi yang terdiri dari banyak komputer.

Secara esensial, dua jenis teknologi yang membuat kriptografi kuantum ini mungkin diimplementasikan adalah peralatan untuk membuat foton tunggal dan peralatan untuk mendeteksinya. Sumber idealnya dinamakan senjata foton (*photon gun*) yang menembakkan foton tunggal berdasarkan permintaan.

Selain contoh di atas, ada banyak aplikasi perbankan yang dapat memakai implementasi kriptografi kuantum ini, misalnya *online banking,* kartu kredit dan lain sebagainya.

5.3. Perbedaan kriptografi kuantum dengan kriptografi lainnya dalam sistem perbankan

Berdasarkan penjelasan-penjelasan di atas, ada beberapa perbedaan antara teknik kriptografi kuantum dengan teknik kriptografi lainnya dalam sistem perbankan.

Kelebihan kriptografi kuantum adalah kemampuannya mendeteksi adanya penyadap kunci. Selain itu, adanya teori fisika kuantum yang membuat keyakinan bahwa kriptografi ini susah dipecahkan. Kriptografi kuantum berhasil memecahkan masalah utama tidak berkembangnya algoritma kriptografi kunci simetri yang disebabkan oleh masalah pendistribusian kunci. Adapun kekurangan kriptografi kuantum adalah peralatannya yang rumit dan mahal. Kriptografi kuantum juga tidak memiliki perlindungan terhadap *man-in-the-middle attack*. Hal ini terjadi karena mengirimkan informasi dengan menggunakan sebuah foton relatif sulit. Walaupun kriptografi ini dapat diandalkan (*reliable*), masih terdapat juga kelemahannya.

Jika dibandingkan dengan algoritma kriptografi lain dalam sistem perbankan, seperti algoritma DES atau RSA, kelebihan algoritma-algoritma ini adalah kuncinya relatif pendek, sehingga memudahkan dalam distribusi kunci. Kekurangannya adalah algoritma-algoritma ini sudah dipecahkan. Selain itu, dalam RSA terdapat kerumitan, yaitu dalam memfaktorkan bilangan besar ke bilangan prima.

5.4 Keandalan kriptografi kuantum dalam sistem perbankan

Nilai jual utama dari kriptografi kuantum adalah keamanan absolut. Namun apakah hal ini dijamin? Bahkan ketika protokol-protokol secara matematis terbukti aman, ternyata susah juga untuk mencapai ketetapan dan implementasi keamanan yang dapat dipercaya. Aplikasi *Quantum Key Distribution* yang nyata juga harus menghadapai dunia nyata. Tidak ada sistem kriptografi kuantum yang benar-benar ideal. Oleh sebab itu, pengujian harus dilakukan untuk memastikan adanya kekurangan dalam komponen kuantum atau komponen lainnya, atau dalam antarmukanya, supaya kerusakan yang lebih besar tidak ditimbulkan. Teknik kriptografi kuantum juga tidak bisa membedakan manakah yang *noise* dan mana yang merupakan penyadapan informasi. Selain itu,

terdapat banyak faktor lain juga yang mempengaruhi, misalnya fiber optik yang digunakan sebagai saluran komunikasi mungkin saja mengalami kerusakan di tengah jalan atau keausan karena lamanya pemakaian.

6. KESIMPULAN

Kriptografi kuantum adalah teknik yang memakai prinsip mekanisme kuantum yang tidak pasti untuk menjamin keamanan distribusi kunci pada kriptografi, khususnya untuk kriptografi kunci simetri. Dalam implementasinya di sistem perbankan, teknik ini dapat dipakai untuk transfer, pemakaian ATM, *online banking,* kartu kredit dan lain sebagainya. Teknik kriptografi kuantum menggunakan fiber optik untuk menyalurkan foton dari pengirim ke penerima.

Perbedaan kriptografi kuantum dengan kriptografi lainnya dalam sistem perbankan dapat dilihat di tabel di bawah ini.

Tabel 1: Perbedaan Kriptografi Kuantum dengan Kriptografi yang lain

Faktor pembeda	Kriptografi kuantum	Kriptografi lain (DES, RSA, dll)
Kerumitan implementasi	Relatif rumit dan mahal	Relatif sederhana dan murah
Keandalan	Dapat diandalkan (aman)	Kurang dapat diandalkan (karena sudah dipecahkan)
Pihak ketiga (penyadap)	Dapat terdeteksi	Sulit terdeteksi
Kemungkinan dipecahkan	Sulit/ hampir tidak bisa dipecahkan kuncinya	Mudah dipecahkan kuncinya
Panjang kunci	Sepanjang pesan aslinya (OTP)	Relatif pendek

Kriptografi kuantum tidak sepenuhnya terjamin dan dapat diandalkan. Ada beberapa faktor yang mempengaruhi keandalan kriptografi kuantum, misalnya foton, fiber optik, dan kemampuan teknik ini untuk membedakan *noise* dan penyadapan.

DAFTAR REFERENSI

[1] Kriptografi dalam Kehidupan Sehari-hari
http://kur2003.if.itb.ac.id/file/Kriptografi%20dalam%20Kehidupan%20Sehari-hari.doc
Tanggal akses: 4 Maret 2010

[2] Is unconditionally secure Quantum Cryptography unbreakable?
http://www.cs.york.ac.uk/nature/workshop/papers/Nagarajan.pdf
Tanggal akses: 4 Maret 2010

[3] Gaya Hidup Kelas Menengah
http://www.hamline.edu/apakabar/basisdata/1996/09/30/0039.html
Tanggal akses: 4 Maret 2010

[4] Bahan Kuliah IF3054
Munir, Rinaldi. 2010. Bahan Kuliah IF3054 Kriptografi. Departemen Teknik Informatika. Institut Teknologi Bandung.

[5] NIST reports measurable success of Advanced Encryption Standard - News Briefs - National Institute of Standards and Technology - Brief Article
http://findarticles.com/p/articles/mi_m0IKZ/is_3_107/ai_90984479/?tag=content;col1
Tanggal akses: 25 Maret 2010

[6] http://www.ittelkom.ac.id/library/index.php?option=com_repository&Itemid=34&task=detail&nim=113020061
Tanggal akses: 25 Maret 2010

[7] Bruce Schneier, *Applied Cryptography*, 2nd edition, Wiley, 1996.

[8] Menezes, A., van Oorschot, P., & Vanstone, S. (1997). *Handbook of Applied Cryptography.* CRC Press.

[9] Financial Cryptography in 7 Layers
http://iang.org/papers/fc7.html
Tanggal akses: 25 Maret 2010

[10] Getting Triple DES compliant - www.atmmarketplace.com
Tanggal akses: 25 Maret 2010

[11] Kriptografi dalam Kehidupan Sehari-hari
http://www.docstoc.com/docs/20504314/Kriptografi-dalam-Kehidupan-Sehari-hari
Tanggal akses: 25 Maret 2010

[12] Tanenbaum, Andrew, Computer Networks, Fourth Edition, Prentice Hall, New Jersey, 2003

[13] http://en.wikipedia.org/wiki/File:ATM_750x1300.jpg
Tanggal akses: 25 Maret 2010

[14] One Time Pad
http://www.cypherspace.org/rsa/otp.html
Tanggal akses: 25 Maret 2010

[15] One-Time-Pad (Vernam's Cipher) Frequently Asked Questions
http://www.ranum.com/security/computer_securi

ty/papers/otp-faq/index.htm#head_whatis
Tanggal akses: 25 Maret 2010

[16] Cryptolecture12
http://www.icg.isy.liu.se/courses/tsit03/en/Cryptolecture12.pdf
Tanggal akses: 25 Maret 2010

[17] Quantum Cryptography
http://www.quantenkryptographie.at/Quantum%20Cryptography%2021%20April%2004.pdf
Tanggal akses: 25 Maret 2010

[18] Quantum cryptography: the key to secure data transfer
http://fibresystems.org/cws/article/magazine/19833
Tanggal akses: 25 Maret 2010

[19] http://upload.wikimedia.org/wikipedia/commons/4/49/Fibreoptic.jpg
Tanggal akses: 25 Maret 2010

[20] Quantum Cryptography: Privacy Through Uncertainty
http://www.csa.com/discoveryguides/crypt/overview.php
Tanggal akses: 25 Maret 2010