PENGANTAR

KRIPTOGRAFIK KUANTUM

Teknik Enkripsi Masa Depan

GRAHA ILMU

Dr. Ir. Saludin Muis, M. Kom

PENGANTAR KRIPTOGRAFIK KUANTUM

Teknik Enkripsi Masa Depan

KRIPTOGRAFIK KUANTUM

Teknik Enkripsi Masa Depan

Oleh : Dr. Ir. Saludin Muis, M.Kom

Edisi Pertama
Cetakan Pertama, 2013

GRAHA ILMU
Ruko Jambusari No. 7A
Yogyakarta 55283
Telp. : 0274-889836; 0274-889398
Fax. : 0274-889057
E-mail : info@grahailmu.co.id

Muis, Saludin, Dr., Ir., M.Kom.

KRIPTOGRAFIK KUANTUM; Teknik Enkripsi Masa Depan/Dr. Ir. Saludin Muis, M.Kom.
- Edisi Pertama – Yogyakarta; Graha Ilmu, 2013
xii + 144, 1 Jil. : 26 cm.

ISBN: 978-979-756-944-0

1. Teknik I. Judul

KATA PENGANTAR

Penulis bersyukur ditengah-tengah kesibukan kerja dapat menyelesaikan penulisan buku ini, dimana penulis dapat membagi sepotong pengetahuan mengenai teknik kriptografik kuantum yang merupakan teknik enkripsi masa depan yang memanfaatkan pengetahuan kuantum atomik yang memiliki karakteristik sangat unik yang sulit dipecahkan.

Penulis berharap pengetahuan yang tercakup dalam buku ini dapat memberikan sebuah ide dasar kepada pembaca yang selanjutnya dapat dikembangkan lebih lanjut untuk aplikasi praktis yang memiliki nilai ekonomis. Tentu pembaca diharapkan memahami pengetahuan dasar ilmu kuantum yang mendasari pembahasan buku ini sehingga dapat menangkap intisari dibalik ide kriptografik kuantum yang diyakini akan merupakan teknik enkripsi di masa mendatang.

Pada kesempatan ini, dari lubuk hati penulis terdalam, penulis mengucapkan terima kasih setulusnya kepada 6 orang yang berperan besar dan merubah perjalanan hidup penulis, yaitu Ibu Saini (Alm), T. Oh Huan (Alm), Albert Ray J, Alexander Rex., Ibu Maria Dwi K ,dan Ibu RajaniTjandra.

-oo0oo-

DAFTAR ISI

KATA PENGANTAR **v**

DAFTAR ISI **vii**

PENDAHULUAN **ix**

BAB 1 TINJAUAN UMUM **1**

BAB 2 KRIPTOGRAFIK KLASIK **7**

2.1 Kerahasiaan Dan Sandi Kunci Rahasia 7
2.2 Otentikasi Kunci Rahasia 14
2.3 Kriptografik Kunci Umum 15
2.4 Kesimpulan 18

BAB 3 TEORI INFORMASI KUANTUM **19**

3.1 Definisi Dasar Dalam Mekanik Kuantum 19
3.2 Qubit Dan Pasangan-Pasangan Qubit 21
3.3 Entropi dan Pengkodean 23
3.4 Kekhususan Informasi Kuantum 24
3.5 Kuantum Optik 25
3.6 Kesimpulan 27

BAB 4 **SISTEM KRIPTO BERDASARKAN DISTRIBUSI KUNCI KUANTUM** 29

4.1 Kanal Otentikasi Klasik 30
4.2 Bagan Enkripsi Kunci rahasia 33
4.3 Menggabungkan Kriptografik Kuantum Dan Klasik 34
4.4 Implementasi Sebuah Kripto Sistem Berdasarkan QKD 37
4.5 Kesimpulan 41

BAB 5 HASIL UMUM DISTILASI KUNCI RAHASIA **43**
5.1 Pendekatan Dua Langkah 43
5.2 Karakteristik-Karakteristik Teknik Distilasi 44
5.3 Distilasi Kunci Rahasia Satu Kali Kerja Terotentikasi 45
5.4 Distilasi Kunci Rahasia Ulang-Ulang Terotentikasi 47
5.5 Distilasi Kunci Rahasia Tidak Terotentikasi 50
5.6 Distilasi Kunci Rahasia Dengan Variabel-Variabel Kontinu 51
5.7 Kesimpulan 52

BAB 6 ANALISIS KEAMANAN UNTUK DISTRIBUSI KUNCI KUANTUM **55**
6.1 Strategi Pengupingan Dan Distilasi Kunci Rahasia 55
6.2 Distilasi Diperoleh Dari Keterlibatan Pemurnian 56
6.3 Aplikasi Protokol GG02 66
6.4 Kesimpulan 80

DAFTAR PUSTAKA **81**

LAMPIRAN A: PROTOKOL BB84 **83**

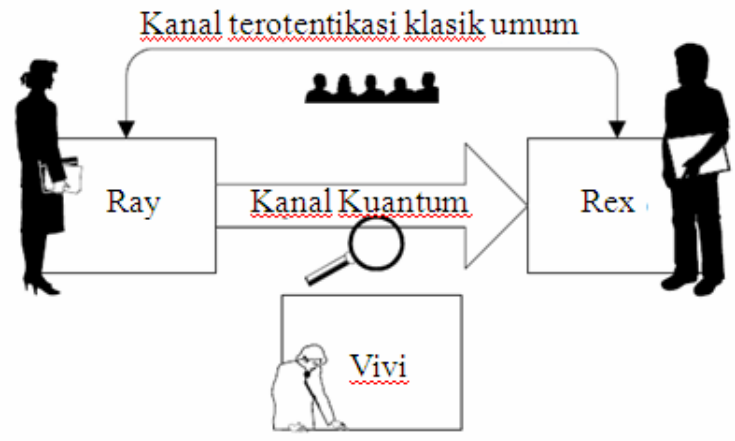
LAMPIRAN B: PROTOKOL GG02 **101**

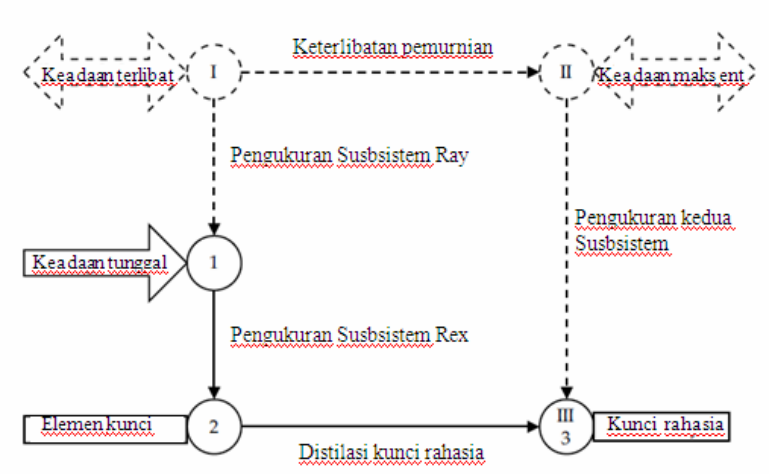
TENTANG PENULIS **115**

-oo0oo-

PENDAHULUAN

Kendala implementasi ide kriptografik kuantum adalah pada pembangkitan sumber foton tunggal (ideal) dan penggunaan foton jamak.banyak yang bersifat koheren lemah (pendekatan, *keadaan koheren adalah sebuah keadaan yang mempunyai fluktuasi kuadratur amplitudo sama sebagai keadaan hampa tetapi yang mungkin mempunyai rata-rata kuadratur amplitudo tidak nol*.) yang dipergunakan untuk membangkitkan kunci rahasia yang dibutuhkan. Dari kedua sumber foton yang mungkin tersebut, dalam implementasi masing-masing ada plus-minusnya secara teknis, misalnya sumber foton jamak yang secara teknis lebih mudah diimplementasikan, namun tidak sebaik dalam hal keamanan dibandingkan sumber foton tunggal. Secara garis besar kedua sumber tersebut dapat diilustrasikan sebagai berikut





Pada gambar, Ray dan Rex adalah dua pihak sah yang berkomunikasi dengan menggunakan kunci kuantum untuk keamanan data dan Vivi adalah pihak yang menguping atau menyadap komunikasi antara pihak-pihak berhak untuk mengetahui kunci rahasia kuantum yang dipergunakan. Secara teknis, ekivalen formal protokol distribusi kunci kuantum dan distilasi kunci rahasianya dengan sebuah protokol keterlibatan pemurnian dapat mengambil dua jalur, yaitu protokol realistik mengikuti lintasan 1-2-3, sedangkan protokol formal mengikuti lintasan I-II-III. Sedangkan garis titik-titik menunjukkan bagian formal, yang tidak harus di implementasikan dalam praktek.

Pembahasan teknik kriptografik kuantum pada buku ini disajikan secara ringkas dan padat dengan titik fokus pada ide kuantum yang melatar-belakangi. Adapun pembagian bab per bab dan lampiran pelengkap adalah sebagai berikut :

Bab 1 berisikan garis besar bagaimana prinsip kerja kriptografik kuantum, pada bab ini pembaca diperkenalkan kepada seperti apa dunia kriptografik kuantum itu bekerja dan merupakan bekal bagi pembaca untuk masuk ke bab-bab selanjutnya.

Pada bab 2, pembaca diingatkan kembali dasar-dasar kriptografik klasik dan dikaitkan dengan ide kriptografik kuantum karena pemahaman pengkodean secara kuantum yang dalam hal ini berupa kunci rahasia maupun engkripsi data komunikasi tidak terlepas dari ide umum pengkodean klasik.

Mulai bab 3 sampai bab 6, pembaca benar-benar dibawa ke dunia bagaimana kriptografik kuantum bekerja. Dimana pada bab 3 berisikan teori informasi kuantum, pembaca disajikan bagaimana ide dibalik mempergunakan keadaan-keadaan kuantum atomik untuk maksud pengkodean kunci rahasia. Seperti Bagan kerja kriptografik pada umum, kriptografik kuantum juga mendistribusikan kunci kuantum antara pemakai berhak, sehingga pada bab 4 disajikan sistem kriptografik berdasarkan distribusi kunci kuantum. Sedangkan bagaimana kedua pihak berhak melakukan enkripsi/pengkodean dan dekripsi/pencacahan data dengan aman dibahas pada bab 5 yang berisikan hasil umum distilasi kunci rahasia.