BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan transmisi data merupakan aspek krusial dalam sistem komunikasi digital modern, terutama untuk menjaga kerahasiaan informasi yang dipertukarkan melalui jaringan terbuka [1, 2]. Transmisi data sendiri merujuk pada proses pengiriman informasi dari satu entitas ke entitas lain melalui media komunikasi seperti jaringan internet, jaringan seluler, maupun infrastruktur berbasis serat optik. Proses ini mencakup pertukaran data dalam berbagai bentuk, mulai dari pesan teks, transaksi keuangan, komunikasi pemerintahan, hingga distribusi data pada sistem komputasi awan (*cloud computing*) dan *Internet of Things* (IoT). Ancaman terhadap keamanan transmisi data terus meningkat, di mana sekitar 22% dari semua pelanggaran data pada 2025 disebabkan oleh penyalahgunaan kredensial (*credential abuse*) yang memungkinkan akses tidak sah ke informasi sensitif. Selain itu, lebih dari 83% pelanggaran data global pada periode yang sama melibatkan data yang kemudian dijual atau disalahgunakan di forum gelap, menunjukkan risiko serius terhadap kerahasiaan dan integritas data yang dikirimkan melalui jaringan [3]. Selama ini, sistem keamanan data banyak bergantung pada algoritma kriptografi klasik untuk melindungi data dari akses tidak sah. Namun, perkembangan teknologi komputasi kuantum menghadirkan ancaman baru terhadap mekanisme keamanan tersebut karena kemampuannya memecahkan permasalahan matematis yang sebelumnya dianggap sulit secara komputasional [4]. Kondisi ini menunjukkan bahwa infrastruktur keamanan data saat ini berpotensi menjadi tidak memadai di masa depan [5].

Dalam praktik sistem komunikasi modern, enkripsi data umumnya dilakukan menggunakan algoritma simetris seperti Advanced Encryption Standard (AES) karena efisiensinya dalam memproses data berukuran besar. Analisis perbandingan antara algoritma kriptografi klasik dan *post-quantum* menunjukkan bahwa mekanisme keamanan berbasis asumsi kesulitan komputasi tidak lagi mampu menjamin keamanan jangka panjang dalam skenario keberadaan komputer kuantum skala besar [6, 7]. Oleh karena itu, diperlukan mekanisme distribusi kunci yang tidak bergantung pada kompleksitas komputasi semata [8-10].

Distribusi kunci merupakan komponen kritis dalam sistem keamanan

transmisi data, karena kerahasiaan data sangat bergantung pada kerahasiaan kunci enkripsi. Pada sistem klasik, proses pertukaran kunci sering dilakukan melalui kanal publik yang rentan terhadap serangan penyadapan atau manipulasi. Sebagian besar mekanisme berbagai protokol pertukaran kunci klasik tidak memiliki kemampuan intrinsik untuk mendeteksi aktivitas intersepsi oleh pihak ketiga selama proses distribusi kunci [11]. Bahkan algoritma yang secara matematis kuat seperti Diffie–Hellman tetap berisiko jika tidak dilengkapi mekanisme autentikasi dan proteksi tambahan [12].

Ancaman yang ditimbulkan oleh komputasi kuantum tidak hanya bersifat teoretis, tetapi juga menjadi perhatian serius dalam pengembangan sistem keamanan masa depan. Algoritma kuantum, seperti Algoritma Shor dan Grover, mampu secara signifikan mengurangi tingkat keamanan kriptografi klasik yang banyak digunakan saat ini, sehingga berpotensi membahayakan kerahasiaan data dan proses distribusi kunci [13, 14]. Kondisi ini menegaskan urgensi pengembangan dan evaluasi mekanisme keamanan yang bersifat tahan terhadap serangan kuantum. Salah satu pendekatan yang banyak dikaji adalah pemanfaatan prinsip mekanika kuantum dalam sistem keamanan komunikasi [15].

Quantum Key Distribution (QKD) menawarkan pendekatan baru dalam distribusi kunci kriptografi dengan memanfaatkan sifat dasar mekanika kuantum [16]. Berbeda dengan metode klasik, QKD tidak bergantung pada asumsi kesulitan komputasi, melainkan pada hukum fisika untuk menjamin keamanan distribusi kunci. Protokol *Quantum Key Distribution* mampu memberikan keamanan bersifat *information-theoretic* yang tidak bergantung pada asumsi komputasi, sehingga secara fundamental tahan terhadap serangan kuantum [17]. Meskipun demikian, tingkat keamanan dan efisiensi sistem QKD sangat dipengaruhi oleh protokol yang digunakan dalam proses distribusi kunci. Protokol BB84 merupakan protokol QKD fundamental yang banyak digunakan sebagai acuan dalam analisis kualitas kunci, khususnya melalui parameter *Quantum Bit Error Rate* (QBER) [18-20].

Keamanan protokol BB84 bergantung pada kemampuannya mendeteksi gangguan selama proses transmisi qubit, baik yang disebabkan oleh noise maupun oleh aktivitas penyadapan. Gangguan tersebut dapat diukur melalui *Quantum Bit Error Rate* (QBER), yang menjadi indikator utama keberadaan *eavesdropper* dalam sistem QKD [21]. Dalam implementasinya, protokol BB84 umumnya diterapkan pada sistem komunikasi berbasis serat optik maupun komunikasi satelit kuantum untuk mendistribusikan kunci kriptografi secara aman antara dua lokasi yang terpisah. Tinjauan terhadap implementasi praktis QKD membuktikan bahwa

berbagai bentuk serangan pada celah keamanan perangkat (*quantum hacking*) akan memengaruhi tingkat kesalahan bit kuantum (QBER) dan memaksa penurunan laju kunci rahasia yang dihasilkan [22]. Dengan demikian, permasalahan utama terletak pada bagaimana mengukur dan menganalisis perubahan nilai QBER sebagai indikator keandalan serta keamanan kunci yang dihasilkan oleh protokol BB84 dalam kondisi adanya gangguan. Analisis terhadap kualitas kunci BB84 melalui metrik seperti QBER menjadi penting untuk mengevaluasi efektivitas protokol ini dalam mendukung keamanan transmisi data.

Berdasarkan permasalahan tersebut, penelitian ini diarahkan untuk mengkaji secara sistematis pengaruh beberapa parameter sistem terhadap kualitas kunci yang dihasilkan oleh protokol BB84 serta implikasinya terhadap keamanan transmisi data. Penelitian dilakukan melalui simulasi proses distribusi kunci BB84 menggunakan bahasa pemrograman Python untuk memodelkan komunikasi kuantum antara pihak pengirim (Alice) dan penerima (Bob). Simulasi ini mempertimbangkan beberapa parameter utama, yaitu jumlah qubit yang dikirimkan, keberadaan penyadap (*eavesdropper*) dengan model serangan *intercept-resend*, serta pengaruh *noise* pada kanal komunikasi kuantum. Evaluasi performa sistem dilakukan dengan menggunakan metrik *Quantum Bit Error Rate* (QBER) untuk mengukur tingkat kesalahan bit selama proses distribusi, *Key Generation Rate* (KGR) untuk menganalisis efisiensi kuantitas kunci hasil penyaringan (*sifting*), serta *Secret Key Rate* (SKR) untuk mengevaluasi laju pembentukan kunci rahasia akhir yang aman setelah memperhitungkan penalti entropi kebocoran informasi. Melalui variasi parameter tersebut, penelitian ini bertujuan untuk menganalisis bagaimana perubahan kondisi komunikasi mempengaruhi kualitas dan keandalan kunci yang dihasilkan oleh protokol BB84. Dengan demikian, diharapkan penelitian ini dapat memberikan gambaran yang lebih komprehensif mengenai performa dan efektivitas protokol BB84 sebagai mekanisme distribusi kunci dalam mendukung keamanan transmisi data.

1.2 Rumusan Masalah

Berdasarkan penjelasan yang telah dipaparkan pada latar belakang, maka rumusan masalah dalam penelitian ini adalah sebagai berikut.

1. Bagaimana keamanan transmisi data dapat dijamin melalui mekanisme pendeteksian ancaman berbasis *Quantum Bit Error Rate* (QBER) pada penerapan protokol BB84?

2. Bagaimana proses distribusi pada protokol BB84 dieksekusi untuk menghasilkan *shared key* yang identik dan tervalidasi antara pihak pengirim dan penerima?

3. Bagaimana tingkat ketahanan kunci yang direpresentasikan oleh metrik *Secret Key Rate* (SKR) pada protokol BB84 saat dihadapkan pada skenario peningkatan *channel noise* dan probabilitas intersepsi (*eavesdropping*)?

1.3 Batasan Permasalahan

Untuk menjaga konsistensi dan ruang lingkup penelitian, batasan permasalahan yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Proses komunikasi dan distribusi kunci dilakukan dalam bentuk simulasi berbasis perangkat lunak, tanpa menggunakan perangkat keras kuantum nyata.

2. Model serangan yang dianalisis dibatasi pada *intercept-resend attack* (*eavesdropping*).

3. Variasi pengujian dilakukan berdasarkan perubahan jumlah qubit yang digunakan dalam proses distribusi kunci, keberadaan eavesdropper, dan noise pada kanal komunikasi.

4. Penelitian ini tidak membahas optimasi performa ataupun pengembangan protokol QKD BB84 ataupun lainnya.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, maka tujuan dari penelitian ini adalah sebagai berikut.

1. Menganalisis mekanisme pendeteksian ancaman berbasis *Quantum Bit Error Rate* (QBER) pada penerapan protokol *Quantum Key Distribution* (QKD) BB84 dalam menjamin keamanan transmisi data.

2. Mendemonstrasikan proses distribusi dan rekonsiliasi basis kuantum pada protokol BB84 untuk menghasilkan *shared key* yang identik dan tervalidasi antara pihak pengirim dan penerima.

3. Mengevaluasi tingkat ketahanan kunci yang direpresentasikan oleh metrik *Secret Key Rate* (SKR) pada protokol BB84 terhadap skenario peningkatan gangguan lingkungan (*channel noise*) dan probabilitas intersepsi (*eavesdropping*).

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut.

1. Memberikan kontribusi kajian ilmiah mengenai pemahaman dan penerapan protokol BB84 dalam skema pengamanan transmisi data, khususnya dalam konteks simulasi *Quantum Key Distribution*.
2. Menjadi referensi bagi peneliti lain dalam mengimplementasikan dan mengevaluasi sistem keamanan data berbasis kombinasi protokol kuantum dan kriptografi simetris.
3. Memberikan gambaran awal mengenai potensi penerapan teknologi *Quantum Key Distribution* sebagai solusi keamanan komunikasi data di masa depan.

1.6 Sistematika Penulisan

Laporan penelitian ini disusun dalam lima bab yang saling berkaitan dan sistematis, guna menjelaskan dasar teori, perancangan sistem, implementasi, hingga evaluasi performa distribusi kunci kuantum menggunakan protokol BB84. Adapun sistematika penulisan dalam penelitian ini adalah sebagai berikut:

1. Bab 1 PENDAHULUAN
   Bab ini menguraikan latar belakang penelitian mengenai permasalahan keamanan transmisi data dan keterbatasan mekanisme distribusi kunci kriptografi klasik. Selain itu, bab ini memaparkan rumusan masalah, batasan penelitian, tujuan penelitian, serta manfaat yang diharapkan dari implementasi Quantum Key Distribution (QKD) berbasis protokol BB84 dalam meningkatkan keamanan komunikasi data.
2. Bab 2 LANDASAN TEORI
   Bab ini menyajikan teori-teori yang menjadi dasar penelitian, meliputi konsep transmisi data dan keamanan komunikasi, enkripsi serta distribusi kunci kriptografi klasik, prinsip dasar komputasi dan kriptografi kuantum, konsep

Quantum Key Distribution (QKD), serta mekanisme protokol BB84. Pada bab ini juga dijelaskan konsep Quantum Bit Error Rate (QBER) sebagai parameter deteksi penyadapan dalam sistem distribusi kunci kuantum.

3. Bab 3 METODOLOGI PENELITIAN

   Bab ini menjelaskan metode penelitian yang digunakan, termasuk perancangan sistem simulasi atau implementasi protokol BB84, skenario komunikasi antara Alice dan Bob, serta model serangan seperti intercept-resend attack. Bab ini juga menjelaskan parameter evaluasi yang digunakan, yaitu *Key Generation Rate* (KGR), *Quantum Bit Error Rate* (QBER), dan *Secret Key Rate* (SKR), serta alur eksperimen yang dilakukan.

4. Bab 4 HASIL DAN DISKUSI

   Bab ini menyajikan hasil implementasi dan pengujian sistem distribusi kunci kuantum menggunakan protokol BB84. Analisis dilakukan berdasarkan nilai KGR untuk mengukur efisiensi pembentukan kunci, QBER untuk mendeteksi keberadaan penyadapan, serta SKR untuk mengukur rasio pembentukan kunci rahasia yang aman. Bab ini juga membahas pengaruh serangan terhadap performa sistem dan efektivitas BB84 dalam menjaga keamanan transmisi data.

5. Bab 5 KESIMPULAN DAN SARAN

   Bab ini merangkum hasil penelitian yang telah dilakukan serta menjawab rumusan masalah berdasarkan analisis yang diperoleh. Selain itu, bab ini memberikan saran untuk pengembangan penelitian selanjutnya, seperti penerapan protokol QKD lainnya, peningkatan model simulasi kanal kuantum, atau integrasi dengan sistem kriptografi modern yang lebih kompleks.