ANALISIS DAMPAK *QUANTUM COMPUTING* TERHADAP KEAMANAN SISTEM KRIPTOGRAFI KONVENSIONAL

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :
HADI RUSWANTO
09011381924142

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

Analisis Dampak Quantum Computing Terhadap Keamanan Sistem Kriptografi Konvensional

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

HADI RUSWANTO
09011381924142

Pembimbing 1 : **Dr. Ahmad Heryanto, S.Kom., M.T.**
NIP. 198701222015041002

Mengetahui
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

AUTHENTICATION PAGE

FINAL TASK

Analysis of the Impact of Quantum Computing on the Security of Conventional Cryptographic Systems

Submitted to Complete One of the Requirements for Obtaining a Bachelor's Degree in Computer Science

By:

HADI RUSWANTO
09011381924142

Supervisor 1 : **Dr. Ahmad Heryanto, S.Kom., M.T.**
NIP. 198701222015041002

Acknowledge
Head of Computer System Department

Dr. Ir. Sukemi, M.T
196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Kamis

Tanggal : 24 Juli 2025

Tim Penguji

1. Ketua : Dr. Ir. Sukemi, M.T. _____

2. Penguji : Kemahyanto Exaudi, M.T. _____

3. Pembimbing 1 : Dr. Ahmad Heryanto, S.Kom., M.T. _____

Mengetahui, 17/8/25

Ketua Jurusan Sistem computer

KEMENTERIAN PENDIDIKAN TINGGI SAINS DAN TEKNOLOGI UNIVERSITAS SRIWIJAYA JURUSAN SISTEM KOMPUTER

Dr. Ir. Sukemi, M.T.

NIP 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Hadi Ruswanto

NIM : 09011381924142

Judul : Analisis Dampak *Quantum Computing* Terhadap Keamanan Sistem Kriptografi Konvensional

Hasil Pengecekan *Software Turnitin*: 17%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, 9 Agustus 2025

Penulis,

Hadi Ruswanto

NIM. 09011381924142

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh, Puji dan syukur penulis ucapkan atas kehadirat Allah SWT. Yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan tugas akhir dengan judul "ANALISIS DAMPAK *QUANTUM COMPUTING* TERHADAP KEAMANAN SISTEM KRIPTOGRAFI KONVENSIONAL"

Pada penyusunan tugas akhir ini tidak terlepas dari peran berbagai pihak yang telah memberikan dukungan doa, semangat, motivasi dan bimbingan pada penulis. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT. yang telah memberikan nikmat Kesehatan dan Kesempatan kepada penulis dalam penyusunan tugas akhir ini.
2. Kedua orang tua tercinta yang selalu memberikan dukungan moral maupun finansial, serta do'a yang tiada hentinya.
3. Kakak - Kakak ku yang selalu memberikan semangat dan do'a.
4. Bapak Dr. Erwin, M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Abdurahman, S. Kom., M. Han. selaku Dosen Pembimbing Akademik.
7. Bapak Dr. Ahmad Heryanto S.Kom., M.T selaku Pembimbing I Tugas Akhir Penulis yang telah meluangkan waktu untuk membimbing dan memberikan motivasi selama pengerjaan Tugas Akhir.
8. Mba Sari Anhar selaku admin yang telah membantu dalam proses administrasi Tugas Akhir Penulis.
9. Teman-teman terdekat selama kuliah yang selalu support.
10. Teman-teman seperjuangan Jurusan Sistem Komputer Unggulan 2019.
11. Seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan semangat serta doa.
12. Almamater

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis dengan senang hati menerima kritik dan saran serta masukkan dari pembaca yang bersifat membangun agar lebih baik lagi dikemudian hari. Penulis berharap semoga laporan ini dapat bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya. Demikian yang dapat penulis sampaikan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, 9 Agustus 2025

Penulis,

Hadi Ruswanto

NIM. 09011381924142

Analisis Dampak *Quantum Computing* Terhadap Keamanan Sistem Kriptografi Konvensional

Hadi Ruswanto (09011381924142)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011381924142@student.unsri.ac.id

ABSTRAK

Kemajuan komputasi kuantum membawa tantangan besar bagi keamanan sistem kriptografi konvensional yang saat ini banyak digunakan, seperti RSA dan ECC, yang bergantung pada kesulitan komputasi faktorisasi bilangan besar dan logaritma diskret. Penelitian ini bertujuan untuk menganalisis dampak dari komputasi kuantum terhadap algoritma kriptografi konvensional dengan menggunakan simulasi algoritma kuantum Shor dan Grover. Metode penelitian dilakukan melalui pendekatan teoritis serta simulasi menggunakan lingkungan kuantum untuk menguji kerentanan algoritma RSA 1024-bit dan 2048-bit serta ECC 256-bit dan 384-bit. Hasil pengujian menunjukkan bahwa algoritma Shor berhasil memfaktorkan kunci RSA 1024-bit dalam waktu yang jauh lebih cepat dibandingkan metode klasik, sedangkan RSA 2048-bit menunjukkan kerentanan yang meningkat seiring proyeksi pertumbuhan qubit di masa depan. Sementara itu, algoritma Grover mempercepat pencarian kunci pada skema ECC secara signifikan, terutama pada ukuran kunci 256-bit, yang menyebabkan penurunan tingkat keamanan setara menjadi separuh bit-length. Penelitian ini juga membandingkan performa pemfaktoran klasik dan kuantum, serta meninjau tantangan teknis implementasi algoritma kuantum dalam skenario dunia nyata. Sebagai strategi mitigasi, direkomendasikan adopsi kriptografi post-kuantum, penggunaan skema hibrida, serta peningkatan panjang kunci kriptografi simetris. Hasil penelitian ini memberikan kontribusi dalam memahami urgensi transisi menuju sistem keamanan yang tahan terhadap serangan kuantum dan dapat menjadi referensi bagi pengembang dan regulator dalam merancang sistem keamanan informasi masa depan.

Kata Kunci: Komputasi kuantum, kriptografi konvensional, algoritma Shor, algoritma Grover, *post-quantum cryptography*.

Analysis of the Impact of Quantum Computing on the Security of Conventional Cryptographic Systems

Hadi Ruswanto (09011381924142)
Computer Systems Department, Faculty of Computer Science, Sriwijaya University
Email: 09011381924142@student.unsri.ac.id

ABSTRACT

The rapid development of quantum computing presents a major challenge to conventional cryptographic systems such as RSA and ECC, which rely on the computational difficulty of factoring large integers and solving discrete logarithm problems. This study aims to analyze the impact of quantum computing on conventional cryptographic algorithms by simulating quantum algorithms namely Shor's and Grover's within a quantum computing environment. The methodology involves theoretical analysis and simulation experiments on RSA 1024-bit and 2048-bit keys, as well as ECC 256-bit and 384-bit keys. The results show that Shor's algorithm can efficiently factor RSA 1024-bit keys significantly faster than classical methods, while RSA 2048-bit also exhibits increasing vulnerability as quantum hardware scales. Furthermore, Grover's algorithm was shown to accelerate brute-force key search on ECC, effectively reducing the security strength of 256-bit keys to the equivalent of 128-bit, posing substantial security concerns. The study compares quantum and classical factoring times, discusses real-world implementation challenges of quantum algorithms, and recommends mitigation strategies such as migrating to post-quantum cryptography, implementing hybrid cryptographic schemes, and increasing symmetric key lengths. The findings underscore the urgency of transitioning to quantum-resistant security systems and offer practical guidance for developers and policymakers preparing for the post-quantum era.

Keywords: Quantum computing, conventional cryptography, Shor's algorithm, Grover's algorithm, post-quantum cryptography.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABLE

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi komputasi telah mengalami perkembangan pesat sejak pertama kali diperkenalkan. Salah satu inovasi paling signifikan dalam beberapa dekade terakhir adalah kemunculan *Quantum Computing* atau komputasi kuantum. *Quantum Computing* menggunakan prinsip-prinsip mekanika kuantum untuk melakukan perhitungan dengan cara yang sangat berbeda dibandingkan dengan komputer konvensional [1]. Teknologi ini memiliki potensi untuk memecahkan masalah-masalah yang sangat kompleks dalam waktu yang jauh lebih singkat daripada komputer klasik.

Quantum Computing didasarkan pada unit dasar yang disebut *qubit* (quantum bit), yang tidak hanya dapat berada dalam keadaan 0 atau 1 seperti bit pada komputer klasik, tetapi juga dalam superposisi kedua keadaan tersebut secara simultan. Selain itu, *qubit* dapat terjerat (*entangled*), memungkinkan korelasi antara *qubit* yang terpisah jarak jauh. Fitur-fitur unik ini memungkinkan *Quantum Computing* untuk melakukan operasi paralel dalam jumlah besar dan menyelesaikan masalah-masalah tertentu yang tidak praktis diselesaikan oleh komputer klasik [2].

Salah satu bidang yang akan sangat terpengaruh oleh kemajuan dalam *Quantum Computing* adalah kriptografi. Kriptografi konvensional, yang menjadi tulang punggung keamanan informasi saat ini, sebagian besar didasarkan pada masalah matematika yang sulit dipecahkan oleh komputer klasik [3]. Misalnya, algoritma RSA (*Rivest-Shamir-Adleman*) dan ECC (*Elliptic Curve Cryptography*) mengandalkan kesulitan faktorisasi bilangan besar dan masalah logaritma diskret untuk menjamin keamanannya [4]. Proses enkripsi dan dekripsi dalam algoritma ini dirancang untuk menjadi sangat sulit dan memakan waktu bagi komputer klasik, sehingga memberikan lapisan keamanan yang kuat bagi data yang dienkripsi.

Namun, algoritma kuantum seperti *Shor's Algorithm* mampu memecahkan masalah faktorisasi dan logaritma diskret dengan efisiensi yang jauh lebih tinggi dibandingkan dengan algoritma klasik. *Shor's Algorithm*, yang ditemukan oleh Peter Shor pada tahun 1994, mampu melakukan faktorisasi bilangan bulat besar dalam waktu polinomial, yang berarti dapat memecahkan algoritma RSA dan ECC dalam waktu yang sangat singkat jika dijalankan pada komputer kuantum yang cukup kuat [5]. Hal ini mengindikasikan bahwa ketika komputer kuantum berskala besar menjadi tersedia, sebagian besar sistem kriptografi konvensional yang digunakan saat ini mungkin menjadi rentan terhadap serangan.

Selain *Shor's Algorithm*, terdapat juga *Grover's Algorithm* yang dapat mempercepat pencarian data dalam database kuantum. Meskipun tidak langsung memecahkan enkripsi, *Grover's Algorithm* dapat secara signifikan mengurangi keamanan algoritma enkripsi simetris dengan mempercepat proses pencarian kunci. Sebagai contoh, algoritma enkripsi simetris seperti AES (*Advanced Encryption Standard*) yang memiliki kekuatan kunci 128-bit dapat dipecahkan dalam waktu yang jauh lebih singkat dengan *Grover's Algorithm*, sehingga mengurangi efektivitas keamanan yang dimilikinya [6].

Untuk menghadapi ancaman yang ditimbulkan oleh *Quantum Computing*, diperlukan pengembangan dalam bidang *post-quantum cryptography* atau kriptografi pasca-kuantum. *Post-quantum cryptography* berfokus pada pengembangan algoritma kriptografi yang tahan terhadap serangan kuantum [7]. Algoritma ini didasarkan pada masalah matematika yang diyakini sulit dipecahkan oleh komputer kuantum, seperti masalah kisi (*lattice problems*), isogenies pada kurva elliptik, dan kode-kode koreksi kesalahan. Dengan demikian, penting bagi para peneliti dan praktisi keamanan informasi untuk memahami dampak potensial dari *Quantum Computing* terhadap infrastruktur keamanan yang ada dan mengembangkan strategi untuk memitigasi risiko yang ditimbulkannya. Penelitian ini bertujuan untuk memberikan pemahaman yang komprehensif tentang dampak *Quantum Computing* terhadap keamanan sistem kriptografi konvensional dan mengidentifikasi solusi yang mungkin.

1.2 Rumusan Masalah

Berikut ini rumusan masalah penelitian Tugas Akhir yang akan dilakukan:

1. Bagaimana prinsip dasar *Quantum Computing* dan Algoritma kuantum beroperasi.
2. Apa dampak dari keberadaan komputer kuantum terhadap keamanan algoritma kriptografi konvensional seperti RSA dan ECC.
3. Strategi atau Langkah apa yang dapat diambil untuk mengamankan sistem kriptografi konvensional dari ancaman yang ditimbulkan oleh *Quantum Computing*.

1.3 Tujuan

Berikut ini merupakan tujuan dari penelitian Tugas Akhir yang dilakukan:

1. Memahami prinsip dasar dan mekanisme operasi *Quantum Computing* serta algoritma kuantum.
2. Menganalisis bagaimana keberadaan komputer kuantum bisa memengaruhi keamanan sistem kriptografi Konvensional.
3. Mengidentifikasi dan mengevaluasi solusi dan strategi yang dapat digunakan untuk mengamankan sistem kriptografi dari ancaman *Quantum Computing*.

1.4 Manfaat

Berikut beberapa manfaat dari penelitian yang dilakukan oleh penulis, diantaranya:

1. Pemahaman yang lebih baik mengenai ancaman yang ditimbulkan oleh *Quantum Computing* terhadap keamanan sistem kriptografi konvensional.
2. Informasi bagi pengembang sistem keamanan mengenai langkah-langkah mitigasi yang dapat diambil untuk meningkatkan keamanan informasi.
3. Memberikan rekomendasi bagi peneliti dan praktisi dalam bidang keamanan informasi mengenai adaptasi dan inovasi yang diperlukan dalam menghadapi era *Quantum Computing*.

1.5 Batasan Masalah

Batasan masalah pada penelitian Tugas Akhir ini adalah sebagai berikut:

1. Penelitian ini hanya akan membahas dampak *Quantum Computing* terhadap algoritma kriptografi konvensional seperti RSA dan ECC, serta beberapa algoritma lain yang umum digunakan.
2. Fokus penelitian adalah pada analisis teoritis dan simulasi dampak *Quantum Computing* terhadap keamanan sistem kriptografi, tidak mencakup implementasi fisik dari komputer kuantum
3. Metode mitigasi yang dibahas akan terbatas pada teknik-teknik yang sedang dalam penelitian dan pengembangan, seperti *post-quantum cryptography*, dan tidak mencakup seluruh spektrum pendekatan keamanan.

1.6 Sistematika Penulisan

Adapun sistematika penulisan dari Tugas Akhir ini sebagai berikut:

BAB I PENDAHULUAN

Bab ini terdapat Latar Belakang penelitian yang dilakukan, Rumusan Masalah, Tujuan dan Manfaat serta metodelogi penelitian dan Sistematika Penelitian.

BAB II TINJAUAN PUSTAKA

Pada bab ini mengkaji teori yang digunakan dalam penelitian untuk mengembangkan hipotesis yang bersumber dari buku, jurnal, artikel ilmiah dan sebagainya.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan tentang metode dan teknik penelitian serta bagaimana langkah dalam menganalisis.

BAB IV HASIL DAN ANALISA

Pada bab ini terdapat penjelasan mengenai penelitian, pembahasan hasil pengujian analisis data dan pembahasan dari hasil penelitian yang merupakan jawaban dari rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan serta saran-saran yang dapat diberikan baik untuk mahasiswa, instansi maupun perusahaan yang berkaitan.

DAFTAR PUSTAKA

[1] A. Dewi Saputri Sistem Informasi, “ANALISIS DAMPAK TEKNOLOGI QUANTUM COMPUTING DALAM KRIPTOGRAFI DAN KEAMANAN INFORMASI.”

[2] G. Parpunguan dan H. Panjaitan, “Sistem Kriptografi Kuantum Perancangan dan Analisis Sistem Kriptografi Kuantum dalam Menghadapi Cyber Attack Quantum.”

[3] L. Clara dan A. Budi, “IMPLEMENTASI METODE ALGORITMA AES PADA PERLINDUNGAN DATA SISTEM LOGIN.”

[4] N. Fadilatul Ilmiyah, “KAJIAN TENTANG KRIPTOSISTEM MCELIECE DALAM MENGHADAPI TANTANGAN KOMPUTER KUANTUM DI ERA REVOLUSI INDUSTRI 4.0,” 2018.

[5] F. Gunadi dan S. R. Widianto, *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS) Perbandingan Data Warehouse Cloud Computing Menggunakan Konvensional Berbasis Kriptografi*.

[6] M. Aria *dkk.*, “Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES,” *Journal on Education*, vol. 05, no. 03, hlm. 6780–6787, 2023.

[7] K. Sebastian Sheva Tjahyana, “Implementasi Algoritma Kriptografi Post-Quantum dalam Sistem Keamanan SSL/TLS.”

[8] D. Volya dan P. Mishra, “State Preparation on Quantum Computers via Quantum Steering,” *IEEE Transactions on Quantum Engineering*, vol. 5, hlm. 1–14, 2024, doi: 10.1109/TQE.2024.3358193.

[9] D. Ferrari, S. Carretta, dan M. Amoretti, “A Modular Quantum Compilation Framework for Distributed Quantum Computing,” *IEEE Transactions on Quantum Engineering*, vol. 4, 2023, doi: 10.1109/TQE.2023.3303935.

[10] M. A. Mimona, M. H. Mobarak, E. Ahmed, F. Kamal, dan M. Hasan, “Nanowires: Exponential speedup in quantum computing,” 15 Juni 2024, *Elsevier Ltd*. doi: 10.1016/j.heliyon.2024.e31940.

[11] S. S. Gill dan R. Buyya, “Transforming Research with Quantum Computing,” *Journal of Economy and Technology*, Jul 2024, doi: 10.1016/j.ject.2024.07.001.

[12] S. Dhar, A. Khare, A. D. Dwivedi, dan R. Singh, “Securing IoT devices: A novel approach using blockchain and quantum cryptography,” *Internet of Things (Netherlands)*, vol. 25, Apr 2024, doi: 10.1016/j.iot.2023.101019.

[13] D. Ukpabi *dkk.*, “Framework for understanding quantum computing use cases from a multidisciplinary perspective and future research directions,” *Futures*, vol. 154, Des 2023, doi: 10.1016/j.futures.2023.103277.

[14] M. Kumar, “Post-quantum cryptography Algorithm’s standardization and performance analysis,” *Array*, vol. 15, Sep 2022, doi: 10.1016/j.array.2022.100242.

[15] H. Kadry, A. Farouk, E. A. Zanaty, dan O. Reyad, “Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security,” *Alexandria Engineering Journal*, vol. 71, hlm. 491–500, Mei 2023, doi: 10.1016/j.aej.2023.03.072.

[16] G. Yalamuri, P. Honnavalli, dan S. Eswaran, “A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats,” dalam *Procedia Computer Science*, Elsevier B.V., 2022, hlm. 834–845. doi: 10.1016/j.procs.2022.12.086.

[17] H. Yalcin, T. Daim, M. M. Moughari, dan A. Mermoud, “Supercomputers and quantum computing on the axis of cyber security,” *Technol Soc*, vol. 77, Jun 2024, doi: 10.1016/j.techsoc.2024.102556.

[18] W. S. Admass, Y. Y. Munaye, dan A. A. Diro, “Cyber security: State of the art, challenges and future directions,” 1 Januari 2024, *KeAi Communications Co.* doi: 10.1016/j.csa.2023.100031.

[19] A. S. R. A. Marco Lucamarini, “ISTITUTO NAZIONALE DI RICERCA METROLOGICA Repository Istituzionale Implementation Security of Quantum Cryptography,” 2025. [Daring]. Tersedia pada: www.etsi.org

[20] Basri Basri, “KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM PERSPEKTIF KEAMANAN DATA DAN KOMPLEKSITAS KOMPUTASI,” 2016, [Daring]. Tersedia pada: http://ejournal.fikom-unasman.ac.id

[21] J. Sasongko, “Pengamanan Data Informasi menggunakan Kriptografi Klasik,” *Jurnal Teknologi Informasi DINAMIK*, vol. X, no. 3, hlm. 160–167, 2005.

[22] M. Kumar, “Quantum Computing and Post Quantum Cryptography,” 2021.

[23] F. Hu *dkk.*, “Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-wave Quantum Computer,” 2019. [Daring]. Tersedia pada: https://www.sciencedirect.com/science/article/pii/S0375960119311569

[24] M. Campagna *dkk.*, “Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges Quantum Safe Cryptography and Security Authors & contributors Quantum Safe Cryptography and Security 2,” 2015. [Daring]. Tersedia pada: www.etsi.org

[25] V. Mavroeidis, K. Vishi, M. D. Zych, dan A. Jøsang, “The Impact of Quantum Computing on Present Cryptography,” Mar 2018, doi: 10.14569/IJACSA.2018.090354.

[26] M. Miftakul Amin, “Implementasi Kriptografi Klasik pada Komunikasi Berbasis Teks”.

[27] A. Firian dan D. E. Octama, “Pengantar Komputasi Modern ‘Mapreduce,’” *Layarinformatika*, 2017.

[28] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, dan J. M. Leimeister, “Quantum computing,” *Electronic Markets*, vol. 32, no. 4, hlm. 2525–2536, 2022, doi: 10.1007/s12525-022-00570-y.

[29] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, dan J. M. Leimeister, “Quantum computing,” *Electronic Markets*, vol. 32, no. 4, hlm. 2525–2536, Des 2022, doi: 10.1007/s12525-022-00570-y.

[30] S. S. Gill dan R. Buyya, “Transforming Research with Quantum Computing,” *Journal of Economy and Technology*, Jul 2024, doi: 10.1016/j.ject.2024.07.001.

[31] D. Boneh dan V. Shoup, “A Graduate Course in Applied Cryptography,” 2017.

[32] G. Brassard, “Brief History of Quantum Cryptography: A Personal Perspective,” 2005. [Daring]. Tersedia pada: http://www.iro.umontreal.ca/~brassard

[33] M. Golec, E. S. Hatay, M. Golec, M. Uyar, M. Golec, dan S. S. Gill, “Quantum cloud computing: Trends and challenges,” *Journal of Economy and Technology*, vol. 2, no. May, hlm. 190–199, 2024, doi: 10.1016/j.ject.2024.05.001.

[34] S. S. Li, G. L. Long, F. S. Bai, S. L. Feng, dan H. Z. Zheng, “Quantum computing,” *Proc Natl Acad Sci U S A*, vol. 98, no. 21, hlm. 11847–11848, 2001, doi: 10.1073/pnas.191373698.

[35] A. Ketha, “The Evolution of Cryptography and a Contextual Analysis of the Major Modern Schemes Historical Overview of Cryptography,” 2023.

[36] D. Boneh dan V. Shoup, “A Graduate Course in Applied Cryptography,” *Crypto.Stanford.Edu*, no. 1, hlm. 1–400, 2015.

[37] A. M. Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data,” *Cryptography and Network Security*, vol. 16, no. 1, hlm. 11, 2017.

[38] J. Pedro Hecht, “Post-Quantum Cryptography: generalized ElGamal cipher over GF(251^8),” *Theoretical and Applied Informatics*, vol. 28, no. 4, hlm. 1–14, Des 2017, doi: 10.20904/284001.

[39] M. A. Jayana, D. Rafael, dan A. A. Rahman, “Implementasi Pengamanan Data Pengarsipan Dengan Metode Algoritma Kriptografi Aes Studi Kasus Pada Bank Bjb Kcp Pasteur Bandung,” *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi dan Teknik*, vol. 4, hlm. 184, 2022, doi: 10.32897/sobat.2022.4.0.1922.