ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Implementasi Kriptografi *Hybrid* RSA dan AES untuk Perlindungan Data Pelanggan pada Aplikasi UMKM Toko dewi badjrah tiga Cikarang Pusat Berbasis *Web*

Implementation of RSA and AES Hybrid Cryptography for Customer Data Protection in Web-Based Store dewi badjrah tiga Cikarang Central UMKM Applications

Michael Andrea Aquino1, Heri Firman Wahyu Hidayat[2], M. Rafli Saputra[3]
[1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa, Bekasi, Indonesia
[1]michaelandrea060@gmail.com, [2]frmanwhid03@gmail.com*, [3]rafliisaputraa13@gmail.com*

Abstract

The rapid adoption of web-based applications by Micro, Small, and Medium Enterprises (UMKM) has significantly increased the volume of customer data processed digitally, including personal identities and transaction records. This condition raises serious security concerns, particularly related to data leakage, unauthorized access, and interception during data transmission. This study aims to design and implement a hybrid cryptographic mechanism that combines the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms to protect customer data in a web-based UMKM application. AES is utilized to encrypt customer data efficiently, while RSA is applied to secure the distribution of the AES secret key, ensuring confidentiality during key exchange. The system is implemented in a web environment and evaluated based on encryption– decryption performance and data confidentiality. The results indicate that the proposed hybrid encryption scheme effectively secures sensitive customer data without significantly impacting system performance, making it suitable for UMKM-scale applications that require both security and efficiency. These findings demonstrate that hybrid cryptography can serve as a practical and reliable solution for enhancing data protection in digital UMKM systems.

Keywords: *UMKM; hybrid cryptography; AES; RSA; data security; web application*

Abstrak

Pemanfaatan aplikasi berbasis *web* pada Usaha Mikro, Kecil, dan Menengah (UMKM) mengalami peningkatan yang signifikan seiring dengan digitalisasi proses bisnis, terutama dalam pengelolaan data pelanggan dan transaksi. Kondisi ini menimbulkan risiko keamanan data, seperti kebocoran informasi pribadi dan akses tidak sah selama proses transmisi data. Penelitian ini bertujuan untuk merancang dan mengimplementasikan mekanisme kriptografi hybrid yang menggabungkan algoritma *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA) dalam melindungi data pelanggan pada aplikasi UMKM berbasis *web*. Algoritma AES digunakan untuk mengenkripsi data pelanggan secara efisien, sedangkan algoritma RSA dimanfaatkan untuk mengamankan proses distribusi kunci AES. Sistem diimplementasikan pada lingkungan aplikasi *web* dan dievaluasi berdasarkan kinerja enkripsi dekripsi serta tingkat kerahasiaan data. Hasil penelitian menunjukkan bahwa penerapan kriptografi *hybrid* mampu meningkatkan keamanan data pelanggan tanpa menurunkan performa sistem secara signifikan. Dengan demikian, skema enkripsi *hybrid* ini dinilai efektif dan layak diterapkan sebagai solusi pengamanan data pada sistem UMKM berbasis digital.

Kata kunci: UMKM; kriptografi *hybrid*; AES; RSA; keamanan data; aplikasi *web*

Pendahuluan

Perkembangan teknologi informasi telah mendorong transformasi digital pada berbagai sektor usaha, termasuk Usaha Mikro, Kecil, dan Menengah (UMKM). Pemanfaatan aplikasi berbasis *web* dalam pengelolaan data pelanggan dan transaksi menjadi solusi utama untuk meningkatkan efisiensi operasional serta kualitas layanan. Namun, peningkatan ketergantungan pada sistem digital juga diikuti oleh meningkatnya risiko keamanan data, khususnya terhadap informasi sensitif pelanggan seperti nama, alamat, dan riwayat transaksi yang diproses dan disimpan secara daring [1]. Tanpa mekanisme perlindungan yang memadai, data tersebut rentan terhadap ancaman penyadapan, manipulasi, maupun akses tidak sah selama proses transmisi maupun penyimpanan.

Dalam konteks aplikasi web UMKM, keamanan data pelanggan menjadi aspek krusial karena kebocoran informasi tidak hanya berdampak pada kerugian finansial, tetapi juga menurunkan tingkat kepercayaan pelanggan terhadap pelaku usaha. Penelitian sebelumnya menunjukkan bahwa transmisi data dalam aplikasi *web* sangat rentan terhadap serangan seperti *man-in-the-middle* dan *eavesdropping* apabila data dikirim dalam bentuk *plaintext* [2]. Risiko tersebut juga termasuk dalam kategori kerentanan kritis aplikasi web sebagaimana dijelaskan dalam standar keamanan OWASP Top 10 [3]. Oleh karena itu, penerapan mekanisme kriptografi menjadi kebutuhan mendasar untuk menjamin kerahasiaan, integritas, dan autentikasi data.

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang menggunakan satu kunci rahasia yang sama dalam proses enkripsi dan dekripsi data. AES dirancang untuk memberikan tingkat keamanan yang tinggi dengan performa yang efisien, sehingga banyak digunakan untuk melindungi data berukuran besar dalam berbagai sistem informasi modern [4], [5]. Algoritma ini bekerja dengan struktur blok dan mendukung panjang kunci 128, 192, dan 256 bit, yang menjadikannya tahan terhadap serangan kriptografi konvensional [3], [6].

Sementara itu, *Rivest Shamir Adleman* (RSA) adalah algoritma kriptografi asimetris yang menggunakan pasangan kunci publik dan kunci privat dalam proses enkripsi dan dekripsi. Keamanan RSA bergantung pada kompleksitas faktorisasi bilangan prima berukuran besar [7], sehingga sangat efektif digunakan untuk mengamankan distribusi kunci dan proses autentikasi. Meskipun memiliki tingkat keamanan yang tinggi, RSA kurang efisien jika digunakan untuk mengenkripsi data dalam jumlah besar karena membutuhkan komputasi yang relatif lebih tinggi [8], [9].

Algoritma kriptografi simetris seperti AES dikenal memiliki keunggulan dalam hal kecepatan dan efisiensi dalam mengenkripsi data berukuran besar [8], sehingga cocok digunakan pada aplikasi yang memproses banyak data pelanggan. Namun, kelemahan utama AES terletak pada proses distribusi kunci rahasia yang berpotensi menjadi celah keamanan apabila tidak diamankan dengan baik [10]. Sebaliknya, algoritma kriptografi asimetris seperti RSA memiliki keunggulan dalam keamanan distribusi kunci, tetapi kurang efisien jika digunakan untuk mengenkripsi data dalam jumlah besar karena membutuhkan komputasi yang lebih tinggi [10], [11].

Untuk mengatasi keterbatasan tersebut, pendekatan kriptografi hybrid yang mengombinasikan algoritma simetris dan asimetris banyak diterapkan dalam penelitian terkini [3], [7], serta direkomendasikan dalam literatur kriptografi modern [12], [13]. Kombinasi AES dan RSA mampu memberikan keseimbangan antara keamanan dan performa sistem. AES digunakan untuk mengenkripsi data pelanggan secara efisien, sedangkan RSA berperan dalam mengamankan distribusi kunci AES.

Berdasarkan permasalahan tersebut, penelitian ini berfokus pada implementasi kriptografi *hybrid* RSA dan AES pada aplikasi UMKM berbasis *web* untuk melindungi data pelanggan. Penelitian ini tidak hanya membahas konsep keamanan data, tetapi juga menyajikan implementasi sistem secara nyata, mulai dari proses input data pelanggan, mekanisme enkripsi, hingga proses dekripsi saat data digunakan kembali. Dengan demikian, penelitian ini diharapkan dapat menjadi acuan praktis bagi pelaku UMKM dalam menerapkan sistem pengamanan data yang aman, efisien, dan sesuai dengan kebutuhan usaha skala kecil.

Metode Penelitian

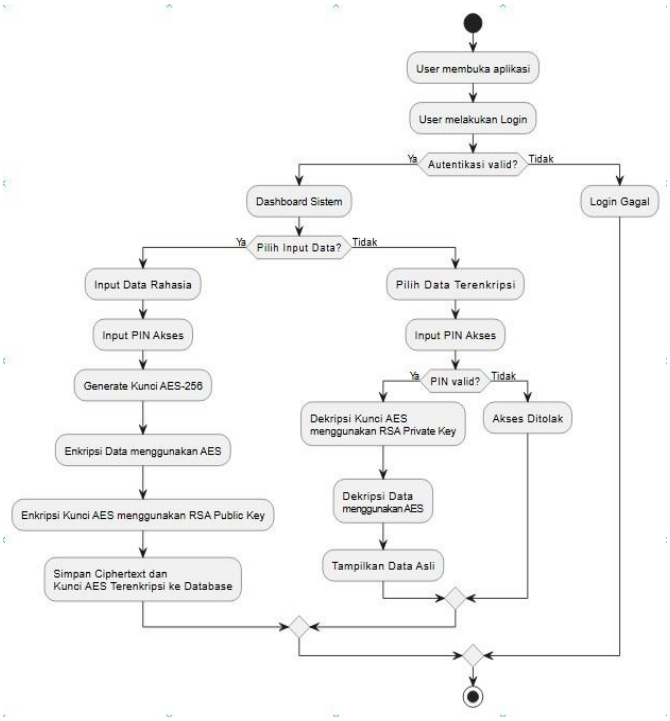
Metode penelitian ini menggunakan pendekatan *Research and Development* (R&D) dengan fokus pada perancangan, implementasi, dan pengujian sistem keamanan data pelanggan pada aplikasi UMKM berbasis *web* melalui penerapan kriptografi *hybrid* RSA dan AES. Pendekatan R&D dipilih karena penelitian ini tidak hanya bertujuan untuk menganalisis fenomena atau konsep keamanan data, tetapi juga menghasilkan produk berupa sistem yang dapat digunakan secara nyata oleh UMKM dengan keterbatasan sumber daya teknologi.

Objek penelitian berupa sistem tersebut yang digunakan untuk mengelola data pelanggan dan transaksi penjualan. Data yang diproses dalam sistem meliputi informasi identitas pelanggan seperti nama dan data transaksi yang bersifat sensitif [1], data pelanggan yang dikirim dan disimpan dalam bentuk *plaintext* pada aplikasi *web* sangat rentan terhadap penyadapan dan akses tidak sah. Oleh karena itu, penelitian ini memfokuskan pengamanan data pada tahap penyimpanan dan pengelolaan data dalam sistem.

Proses pengembangan sistem dilakukan melalui beberapa tahapan utama yang meliputi analisis kebutuhan, perancangan sistem, implementasi, dan pengujian. Pada tahap analisis kebutuhan, dilakukan identifikasi jenis data pelanggan yang perlu dilindungi serta potensi risiko keamanan pada aplikasi UMKM. Tahap perancangan sistem mencakup perancangan alur enkripsi dan dekripsi data, serta integrasi algoritma kriptografi ke dalam sistem aplikasi web. Selanjutnya, tahap implementasi dilakukan dengan menerapkan algoritma kriptografi *hybrid* RSA dan AES ke dalam modul pengolahan data pelanggan.

Mekanisme kriptografi yang digunakan adalah skema *hybrid* dengan mengombinasikan algoritma *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA). Algoritma AES digunakan untuk mengenkripsi data pelanggan karena memiliki performa yang cepat dan efisien dalam menangani data berukuran relatif besar[14]. Data pelanggan yang dimasukkan melalui antarmuka aplikasi akan dienkripsi menggunakan kunci rahasia AES sebelum disimpan ke dalam basis data. Untuk mengamankan distribusi kunci AES, algoritma RSA digunakan untuk mengenkripsi kunci AES menggunakan kunci publik, sehingga kunci tidak tersimpan atau dikirimkan dalam bentuk asli[15].

Alur kerja sistem dimulai dari proses input data pelanggan pada aplikasi UMKM berbasis *web*. Data tersebut kemudian dienkripsi menggunakan algoritma AES, dan hasil enkripsi disimpan ke dalam basis data dalam bentuk *ciphertext*. Kunci AES yang digunakan akan diamankan menggunakan algoritma RSA. Pada saat data dibutuhkan kembali, sistem melakukan proses dekripsi dengan terlebih dahulu mendekripsi kunci AES menggunakan kunci privat RSA, kemudian menggunakan kunci AES tersebut untuk mengembalikan data ke bentuk semula[3], [7]. Untuk memperjelas tahapan proses yang dilakukan oleh sistem, alur kerja tersebut direpresentasikan dalam bentuk *flowchart* sebagaimana ditunjukkan pada Gambar 1.



Gambar 1 Flowchart Sistem Keamanan Data Pelanggan Menggunakan Kriptografi Hybrid RSA dan AES

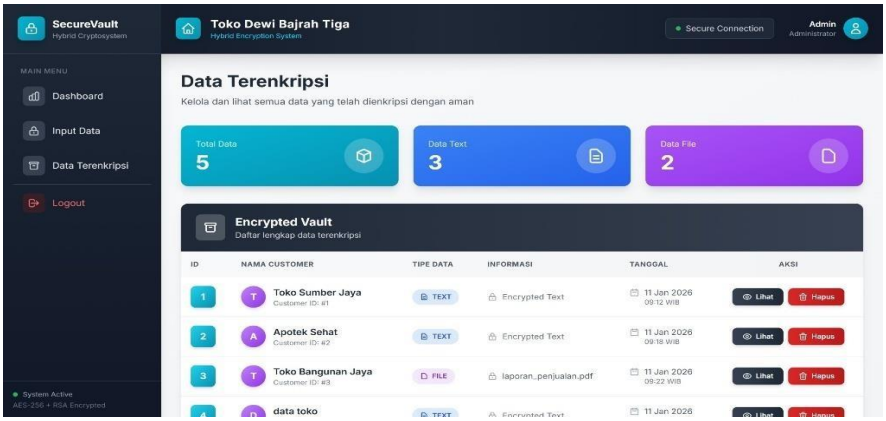
Sistem keamanan data pada aplikasi UMKM ini menggunakan mekanisme kriptografi hybrid dengan mengombinasikan algoritma AES-256 dan RSA-2048. Pemilihan AES-256 didasarkan pada rekomendasi standar keamanan modern yang ditetapkan oleh NIST [9], sedangkan penggunaan RSA-2048 mengacu pada rekomendasi ukuran kunci kriptografi yang dinilai aman terhadap serangan brute force dan faktorisasi modern [15]. Kombinasi ini dirancang untuk memberikan tingkat keamanan tinggi dengan efisiensi komputasi yang tetap sesuai untuk skala UMKM.

Pengujian sistem dilakukan melalui serangkaian skenario fungsional untuk memastikan bahwa mekanisme enkripsi dan dekripsi berjalan sesuai dengan perancangan. Pengujian meliputi simulasi input data pelanggan, verifikasi isi basis data untuk memastikan data tersimpan dalam bentuk *ciphertext*, serta pengujian proses dekripsi untuk memastikan data dapat ditampilkan kembali secara benar. Selain itu, dilakukan pengukuran waktu proses enkripsi dan dekripsi untuk memastikan bahwa penerapan kriptografi *hybrid* tidak menurunkan efisiensi dan kenyamanan penggunaan sistem. Pendekatan pengujian ini bertujuan untuk membuktikan bahwa sistem yang dikembangkan mampu memberikan perlindungan data yang efektif sekaligus tetap sesuai dengan kebutuhan operasional UMKM.

Hasil dan Pembahasan

Implementasi kriptografi *hybrid* RSA dan AES pada aplikasi UMKM berbasis *web* berhasil direalisasikan dalam sebuah sistem prototipe yang dikembangkan untuk mendukung pengamanan data pelanggan. Sistem ini diterapkan pada studi kasus UMKM *Toko Dewi Bajrah Tiga* dan dirancang dengan antarmuka yang sederhana agar mudah digunakan oleh pelaku usaha skala kecil. Melalui sistem ini, data pelanggan yang dimasukkan tidak lagi diproses atau disimpan dalam bentuk *plaintext*, melainkan dienkripsi sebelum disimpan ke dalam basis data, sehingga risiko kebocoran data dapat diminimalkan.

Hasil implementasi sistem ditunjukkan pada Gambar 2, yang menampilkan halaman pengelolaan data terenkripsi (*Encrypted Vault*). Pada tampilan tersebut terlihat bahwa data pelanggan yang telah diproses oleh sistem disimpan dalam bentuk data terenkripsi dan hanya dapat diakses melalui mekanisme yang sah. Hal ini membuktikan bahwa sistem mampu mengelola data pelanggan secara aman serta memisahkan data asli dengan data hasil enkripsi



Gambar 2 Tampilan Halaman Data Terenkripsi pada Sistem Keamanan Data UMKM

Gambar menunjukkan antarmuka sistem pengelolaan data terenkripsi (*Encrypted Vault*) yang menampilkan daftar data pelanggan yang telah dienkripsi menggunakan algoritma AES, dengan pengamanan kunci melalui algoritma RSA. Informasi yang tersimpan tidak dapat dibaca secara langsung dan hanya dapat diakses melalui proses dekripsi yang valid.

Hasil enkripsi data pelanggan menggunakan algoritma AES menghasilkan data dalam bentuk *ciphertext* yang tidak dapat dipahami secara langsung. Algoritma AES dikenal memiliki performa tinggi dalam melindungi data berbasis teks, sehingga sangat sesuai digunakan pada aplikasi UMKM yang memproses data pelanggan secara rutin dan berulang. Penerapan AES dalam sistem ini membuktikan bahwa proses enkripsi dapat dilakukan secara efisien tanpa mengganggu kinerja aplikasi.

Selain pengamanan data, sistem juga menerapkan pengamanan kunci menggunakan algoritma RSA-2048. Kunci rahasia AES yang dihasilkan tidak disimpan dalam bentuk asli, melainkan terlebih dahulu dienkripsi menggunakan kunci publik RSA sebelum disimpan atau digunakan dalam sistem. Dengan mekanisme ini, meskipun pihak tidak berwenang berhasil mengakses basis data, kunci AES tetap tidak dapat dimanfaatkan tanpa kunci privat RSA. Pendekatan ini memperkuat keamanan sistem secara keseluruhan.

Untuk memperjelas hasil implementasi enkripsi, Tabel 1 menyajikan perbandingan antara data pelanggan sebelum enkripsi dan data setelah dienkripsi menggunakan algoritma AES.

Tabel 1 Perbandingan Data Pelanggan Sebelum dan Sesudah Enkripsi

No	Jenis Data	Sebelum Enkripsi	Sesudah Enkripsi (AES)
1	Nama Pelanggan	Rafli Saputra	b'gAAAAABpUleWC5tznQ0ATJfQmaQpac3bFkotYlBu8g-eq7jLbVNKBQvicTNpS_P4DkaJErBUVp76V5JxURA5i3sEdDc6XUK0KA=='
2	Nama Pelanggan	Firman	b'gAAAAABpUlfK4GCsCRf8pn7sj6nAiWMgvxp6by7QV-fN1rY7YA6aFZCYwqE-s6AF7cdntq8qko68-iT86xnHGsIU3SI-E91Nxg=='
3	Nama Pelanggan	Michael	b'gAAAAABpUlh81Tr7_YImcxyhcSwjjNUTPY_EvZNtbWScmUV0Bl4eORmrwduZQjBtQA6zyaqIef2WHYvCGYDRgmUtiryH11yfdw=='

Catatan: *Ciphertext* ditampilkan dalam *format byte string* Python (b'...') setelah proses enkripsi menggunakan algoritma AES-256 dengan mode CBC dan padding PKCS#7.

Pengujian dekripsi dilakukan untuk memastikan bahwa data yang telah dienkripsi dapat dikembalikan ke bentuk semula secara akurat. Hasil pengujian menunjukkan bahwa proses dekripsi tidak menyebabkan kehilangan data atau distorsi informasi. Verifikasi dilakukan secara manual melalui perbandingan langsung antara data input dan data hasil dekripsi. Hasil ini selaras dengan penelitian sebelumnya yang menyatakan bahwa skema kriptografi *hybrid* mampu menjaga integritas data selama proses enkripsi dan dekripsi.

Dari sisi performa, sistem menunjukkan waktu pemrosesan yang efisien. Proses enkripsi AES berlangsung hampir secara *real-time*, sedangkan algoritma RSA hanya digunakan untuk mengamankan kunci AES sehingga tidak menimbulkan beban komputasi yang signifikan terhadap sistem. Temuan ini konsisten dengan penelitian sebelumnya yang menyimpulkan bahwa kriptografi *hybrid* mampu mencapai keseimbangan optimal antara tingkat keamanan dan efisiensi sistem.

Kesimpulan

Secara keseluruhan, hasil implementasi menunjukkan bahwa skema kriptografi *hybrid* berbasis RSA dan AES dapat diterapkan secara efektif pada aplikasi UMKM berbasis *web*. Sistem prototipe yang dikembangkan tidak hanya mampu meningkatkan keamanan data pelanggan melalui mekanisme enkripsi data (menggunakan AES) dan pengamanan kunci (menggunakan RSA) yang terintegrasi, tetapi juga dirancang dengan antarmuka yang sederhana, responsif, serta ringan secara komputasi. Karakteristik tersebut membuat sistem sangat sesuai dengan kebutuhan UMKM yang umumnya memiliki keterbatasan sumber daya teknis maupun sumber daya manusia.

Dengan demikian, penelitian ini menegaskan bahwa pendekatan kriptografi *hybrid* bukan hanya bersifat teoritis, melainkan merupakan solusi praktis dan siap diadopsi untuk mendukung transformasi digital UMKM yang aman. Sistem yang dikembangkan dapat dijadikan sebagai acuan implementatif bagi pelaku usaha skala kecil dalam melindungi data pelanggan, memenuhi prinsip privasi digital, serta meningkatkan kepercayaan pengguna terhadap layanan berbasis *web* yang mereka sediakan.

Daftar Rujukan

[1] H. Putri, L. Virna, T. Febrianti, and T. Sutabri, "MIFORTEKH (Jurnal Manajemen Informatika & Teknologi) Pengamanan Data Transmisi Aplikasi Web Menggunakan Algoritma Kriptografi RSA: Studi Kasus dan Analisis," vol. 5, no. 1, 2025, [Online]. Available: https://https//journal.stiestekom.ac.id/index.php/mifortekh

[2] Y. Bimantoro, R. Titi, and K. Sari, "ENKRIPSI DATA MENGGUNAKAN RSA & AES PADA APLIKASI INSTANT MESSAGING BERBASIS MOBILE," *Jurnal Teknik Informatika*, vol. 14, no. 2, 2021, doi: 10.15408/jti.v14i2.23469.

[3] R. S. Durge and V. M. Deshmukh, "Securing Cloud Data: A hybrid encryption approach with RSA and AES for enhanced security and performance," *Journal of Integrated Science and Technology*, vol. 13, no. 3, 2025, doi: 10.62110/SCIENCEIN.JIST.2025.V13.1060.

[4] Z. Fadilah Azhar, M. Fatiha, A. Vidya Kusumah, D. Izza Al-Din Noor, and M. Zaky Afrilliansyah, "Pengamanan Data Konsumen E-Commerce menggunakan Hybrid Cryptosystem dalam Lingkungan Big Data."

[5] A. Hermawan, E. Iman, and H. Ujianto, "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," vol. 5, no. 2, 2021, doi: 10.30743/infotekjar.v5i2.3585.

[6] L. B. Rivera, J. A. Bay, E. R. Arboleda, M. R. Pereña, and R. M. Dellosa, "Hybrid Cryptosystem Using RSA, DSA, Elgamal, And AES," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 8, no. 10, 2019, [Online]. Available: www.ijstr.org

[7] S. J. Saydahd, R. K. Muhammed, S. A. Hassan, and A. M. Aladdin, "A Comparative Performance Evaluation of Hybrid Encryption Techniques Using ECC, RSA, AES, and ChaCha20 for Secure Data Transmission," *Iraqi Journal of Industrial Research*, vol. 12, no. 2, pp. 157–172, Dec. 2025, doi: 10.53523/ijoirVol12I2ID598.

[8] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Harlow, U.K.: Pearson, 2017.

[9] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[11] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption," in *Advances in Cryptology — EUROCRYPT '94*, Lecture Notes in Computer Science, vol. 950. Berlin, Germany: Springer, 1995, pp. 92–111.

[12] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography. 2020. [Online]. Available: https://crypto.stanford.edu/~dabo/cryptobook/

[13] S. Goldwasser and M. Bellare, *Lecture Notes on Cryptography*. Cambridge, MA, USA: MIT, 2008.

[14] A. K. Lenstra and E. R. Verheul, "Selecting Cryptographic Key Sizes," *Journal of Cryptology*, vol. 14, no. 4, pp. 255–293, 2001.

[15] OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," 2021. [Online]. Available: https://owasp.org/www-project-top-ten/