88/S/TEKKOM-KCBR/PK.03.08/22/AGUSTUS/2025

PENGEMBANGAN APLIKASI *CHATTING MOBILE* MENGGUNAKAN KOMBINASI ALGORITMA RC4 DAN *CAESAR CIPHER* UNTUK PENGAMANAN PESAN

SKRIPSI

diajukan untuk memenuhi sebagian syarat
Untuk memperoleh gelar Sarjana Teknik Program Studi Teknik Komputer

Oleh:
Muhammad Tiar Zuhairmawan
2106342

PROGRAM STUDI S1 TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2025

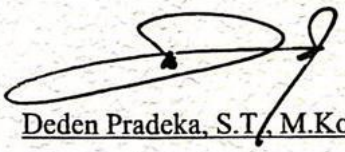
HALAMAN PENGESAHAN SKRIPSI

MUHAMMAD TIAR ZUHAIRMAWAN

PENGEMBANGAN APLIKASI *CHATTING MOBILE* MENGGUNAKAN KOMBINASI ALGORITMA RC4 DAN *CAESAR CIPHER* UNTUK PENGAMANAN PESAN

Disetujui dan Disahkan Oleh Pembimbing:

Pembimbing 1



Deden Pradeka, S.T., M.Kom.

NIP.920200419890816101

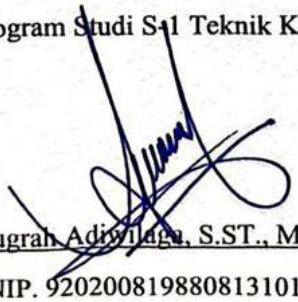
Pembimbing 2

Zahra Khaerunnisa, S.Pd., M.Cs.

NIP.199411112024062001

Mengetahui,

Ketua Program Studi S-1 Teknik Komputer



Anugrah Adiwilaga, S.ST., M.T.

NIP. 920200819880813101

PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Muhammad Tiar Zuhairmawan

NIM : 2106342

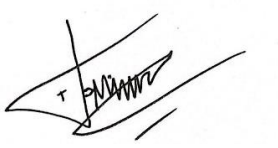
Program Studi : Teknik Komputer

Judul Karya : Pengembangan Aplikasi *Chatting Mobile* Menggunakan Kombinasi Algoritma RC4 dan *caesar cipher* untuk Pengamanan Pesan

Dengan ini saya menyatakan bahwa karya tulis ini merupakan hasil kerja saya sendiri. Saya menjamin bahwa seluruh isi karya ini baik, baik sebagian maupun keseluruhan, bukan merupakan plagiarisme dari karya orang lain, kecuali pada bagian yang telah dinyatakan dan disebutkan sumbernya dengan jelas.

Jika di kemudian hari ditemukan pelanggaran terhadap etika akademi atau unsur plagiarisme, saya bersedia menerima sanksi sesuai peraturan yang berlaku di Universitas Pendidikan Indonesia

Kabupaten Bandung, 24 Agustus 2025



Muhammad Tiar Zuhairmawan

KATA PENGANTAR

Dengan penuh rasa syukur kepada Allah SWT atas rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi yang berjudul "Pengembangan Aplikasi *Chatting Mobile* Menggunakan Kombinasi Algoritma RC4 dan *Caesar Cipher* untuk Pengamanan Pesan " Skripsi ini diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik (S.T) pada Program Studi Teknik Komputer, Kampus UPI di Cibiru, Universitas Pendidikan Indonesia.

Penelitian ini dapat diselesaikan dengan sebaik-baiknya berkat dukungan, bantuan, serta doa dari berbagai pihak. Oleh karena itu, dengan segala hormat dan rasa terima kasih yang tulus, penulis menyampaikan penghargaan sebesar-besarnya kepada:

1. Bapak Deden Pradeka, S.T., M.Kom., selaku Pembimbing I dan Pembimbing akademik, atas segala bimbingan, nasihat, dan dukungan yang diberikan baik dalam penyusunan skripsi maupun selama masa studi.
2. Ibu Zahra Khaerunnisa, S.Pd., M.Cs., selaku pembimbing II, yang senantiasa sabar dan selalu memberikan motivasi selama membimbing penulis selama penyelesaian skripsi.
3. Kedua Orang Tua tercinta dan kakak Hani Nurul Aisha, yang senantiasa memberikan doa, semangat, dan nasihat dalam setiap langkah penulis. Segala pengorbanan dan kasih sayang yang diberikan menjadi kekuatan dalam penyelesaian studi.
4. Seluruh civitas akademika UPI Kampus Cibiru, khususnya para dosen dan staf yang telah memberikan ilmu, arahan, serta fasilitas yang mendukung kelancaran studi dan penelitian ini.
5. Rekan-rekan mahasiswa Teknik Komputer, yang telah menjadi teman seperjuangan selama masa studi, berbagi ilmu, pengalaman, serta semangat dalam menghadapi berbagai tantangan akademik.
6. Keluarga Prasto Sugito, yang senantiasa sabar, mendoakan, dan memberikan semangat maupun motivasi dalam setiap langkah penulis.
7. Syahla Ismah Aprilia, yang telah menjadi pasangan dan senantiasa memberikan motivasi, dan semangat dalam menyelesaikan penelitian ini.

PENGEMBANGAN APLIKASI *CHATTING MOBILE* MENGGUNAKAN KOMBINASI ALGORITMA RC4 DAN *CAESAR CIPHER* UNTUK PENGAMANAN PESAN

Muhammad Tiar Zuhairmawan

2106342

ABSTRAK

Perkembangan teknologi komunikasi digital, khususnya aplikasi *chatting* berbasis mobile, menuntut sistem keamanan yang mampu melindungi kerahasiaan dan integritas data. Penelitian ini mengembangkan aplikasi chatting berbasis Android yang menerapkan skema enkripsi *hybrid* menggunakan kombinasi algoritma RC4 dan *Caesar Cipher*. Sistem dibangun dengan *framework Flutter* dan *Firebase* sebagai *backend*, serta mengadopsi pendekatan *end-to-end encryption*, di mana proses enkripsi dan dekripsi sepenuhnya dilakukan di sisi pengguna. Pengembangan dilakukan dengan metode *Design and Development* (D&D) yang meliputi tahap perancangan, implementasi, dan pengujian. Evaluasi fungsional menunjukkan bahwa aplikasi mampu mengenkripsi seluruh lalu lintas komunikasi secara efektif, sehingga tidak dapat diakses oleh pihak ketiga, sebagaimana dibuktikan melalui analisis jaringan menggunakan Wireshark. Selain itu, uji statistik dengan korelasi Pearson terhadap 21 sampel data menunjukkan nilai rata-rata -0,014 dengan rentang -0,148 hingga +0,097, yang mengindikasikan bahwa *ciphertext* tidak memiliki hubungan linier yang dapat diprediksi dengan *plaintext*. Hasil ini menegaskan bahwa kombinasi algoritma RC4 dan *Caesar Cipher* mampu menghasilkan enkripsi yang kuat dan acak, serta layak diterapkan untuk meningkatkan keamanan komunikasi digital dalam aplikasi *mobile*.

Kata kunci: aplikasi *chatting*, keamanan data, RC4, *Caesar Cipher*, enkripsi *hybrid*

DEVELOPMENT OF MOBILE CHATTING APPLICATION USING RC4 AND CAESAR CIPHER ALGORITHM COMBINATION FOR MESSAGE SECURITY

Muhammad Tiar Zuhairmawan

2106342

ABSTRACT

The development of digital communication technology, particularly mobile-based chatting applications, demands security systems capable of protecting data confidentiality and integrity. This research develops an Android-based chatting application that implements a hybrid encryption scheme using a combination of RC4 and Caesar Cipher algorithms. The system is built with Flutter framework and Firebase as backend, adopting an end-to-end encryption approach where encryption and decryption processes are entirely performed on the user side. Development was conducted using the Design and Development (D&D) method, encompassing design, implementation, and testing phases. Functional evaluation demonstrates that the application can effectively encrypt all communication traffic, making it inaccessible to third parties, as evidenced through network analysis using Wireshark. Additionally, statistical testing using Pearson correlation on 21 data samples shows an average value of -0.014 with a range from -0.148 to +0.097, indicating that the ciphertext has no predictable linear relationship with the plaintext. These results confirm that the combination of RC4 and Caesar Cipher algorithms can produce strong and random encryption, making it suitable for enhancing digital communication security in mobile applications.

Keywords*: chatting application, data security, RC4, Caesar Cipher, hybrid encryption*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PERSAMAAN

DAFTAR PUSTAKA

Abdillah, R., Trinoto, A. A., & Himawan, I. (2023). Static Analysis Using Mobile Security Framework For Smart Home Appliances. *Journal of Information System, Applied, Management, Accounting and Research*, *7*(3), 760–765.

Afzal, A., Hussain, M., Saleem, S., Shahzad, M. K., Ho, A. T. S., & Jung, K.-H. (2021). Encrypted network traffic analysis of secure instant messaging application: A case study of signal messenger app. *Applied Sciences*, *11*(17), 7789.

Almassri S, R. A. R. T. S. H. K. (2023). *Enhancing Mobile Security through a Comprehensive Development Package*. https://doi.org/https://doi.org/10.13140/RG.2.2.22414.54086

AlQahtani, A. A. S. (2025). Key Derivation: A Dynamic PBKDF2 Model for Modern Cryptographic Systems. *Cryptography*, *9*(2), 39.

Alsuwaiedi, H. K. A., & Rahma, A. M. S. (2023). Review of Key Derivation Functions in Cryptographic Systems. *Al-Qadisiyah Journal of Pure Science*, *28*(1), 12.

Alvian Haz, A. (2024). Analisis Keamanan Pesan Teks Menggunakan Kriptografi Hybrid CBC dan RC4. *Jurnal Sarjana Teknik Informatika*, *12*(2), 70–80. https://doi.org/10.12928/jstie.v12i2.26334

Andrea, K., Wardana, A., Wanandi, B. S., & Ikhwan, A. (2023). Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp. *Jurnal Penelitian Dan Pengkajian Ilmiah Eksakta*, *2*(1), 6–11.

Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *Jurnal Teknologi Sistem Informasi*, *4*(2), 394–405.

Arinski, A. W., Wahdini, R., Anggraini, F., Khairani, F., & Sirait, M. T. (2023). Implementasi Algoritma Caesar Cipher Untuk Keamanan Data Anggota Perpustakaan Di Universitas Xyz. *JURNAL SITEBA*, *2*(1), 34–41.

Cahyono, D., Fahrudin, R., & Sinclair, A. (2024). Pentingnya Edukasi dalam Mengatasi Keamanan Data Mobile Banking di Indonesia: The Importance of Education in Overcoming Mobile Banking Data Security in Indonesia. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *3*(1), 81–89.

Chuah, C. W., Alawatugoda, J., & Arbaiy, N. (2024). On Constructing a Secure and Fast Key Derivation Function Based on Stream Ciphers. *International Journal of Advanced Computer Science and Applications*.

Darmawan, R. (2023). Perancangan Aplikasi Kriptografi Menggunakan Algoritma RC4 (Rivest Code 4) Untuk Mengamankan Pesan Email di PT CREATIFACTORY. *OKTAL: Jurnal Ilmu Komputer dan Science*, *2*(3), 740–753.

Dhita, R. L., & Faulina, S. T. (2023). Wisnumurti,"Rancang Bangun Aplikasi Layanan Pengaduan Pada Dinas Pendidikan Kabupaten Oku Berbasis Android Menggunakan Android Studio,." *J. Inform. dan Komput*, *14*(2), 25–35.

Eko, A., & Informatika, S. (2023). Keamanan Pesan Teks Dengan Metode Enkripsi Dan Dekripsi Menggunakan Algoritma Rsa (Rivest Shamir Adleman) Berbasis Android. *Teknologi Pintar. org*, *3*(2), 1.

Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceedings of Informing Science & IT Education Conference (InSITE)*, *10*(10), 107–117.

Fahlevvi, M. R., Harhari, N. S., & Ariandi, W. (2025). Implementasi Algoritma Blowfish untuk Pengamanan Data pada Aplikasi Pengelolaan Kelompok Tani di Kecamatan Dawuan. *JURNAL ILMIAH INFORMATIKA*, *13*(01), 55–61.

Fahruroji, R. T., Wardhani, D. R., & Rahmawan, F. (2024). Sistem Enkripsi Dokumen Menggunakan Metode Rc4 Dan Base64 Pada Justicia Law Firm & Associates. *Semnas Ristek (Seminar Nasional Riset dan Inovasi Teknologi)*, *8*(01).

Faqih, A., Voutama, A., & Saputra, I. (2025). Rancang Bangun Aplikasi Mobile Untuk Pemesanan Tiket Wisata Berbasis Flutter. *Jurnal Informatika dan Teknik Elektro Terapan*, *13*(2).

Fridayanthie, E. W., Haryanto, H., & Tsabitah, T. (2021). Penerapan metode prototype pada perancangan sistem informasi penggajian karyawan (persis gawan) berbasis web. *Jurnal Khatulistiwa Informatika*, *23*(2), 472897.

Gunadi, R. J., Tanone, R., & Beeh, Y. R. (2020). Penerapan firebase cloud storage pada aplikasi mobile android untuk melakukan penyimpanan image lahan pertanian. *Jurnal Teknologi Informasi*, *4*(2), 282–291.

Hasanah, A., Tahir, M., Nisa' Salsabila, F., Aprilia, E. N., Sofiyah, A., Septiyawati, P., & Chilyani, D. (2023). Implementasi Algoritma Caesar Cipher untuk Pengamanan Pesan Menggunakan Java NetBeans. *Digital Transformation Technology (Digitech) | e*, *3*(1). https://doi.org/10.47709/digitech.v3i1.2305

Hendra, H., Awan, A., Waisen, W., Wilianto, W., & Yudi, Y. (2024). Memperkuat Autentikasi dan Integritas Data REST-API Menggunakan Token HMAC SHA-256. *Jurnal Minfo Polgan*, *13*(2), 2189–2197.

Ihsan, I. M., Fauzi, A., & Khair, H. (2024). Application of Cryptography and Steganography Techniques to Improving the Security of Text Messages with RC4 Algorithm and MSB Method. *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, *4*(1), 544–549.

Iswandi, A. A., Ngemba, H. R., Hendra, S., Ulhaq, M. N. D., Iswandi, A., Ngemba, H., Hendra, S., Syahrullah, S., & Noval Daffa Ulhaq, M. (2024). *Implementasi Algoritma RC4 Pada Sistem Informasi Pelaporan DUKCAPIL Provinsi Sulawesi Tengah*.

Juniarmi, I. (2024). Analisis Keamanan Data pada Aplikasi Chatting Menggunakan Enkripsi End-to-End. *Technologia Journal: Jurnal Informatika*, *1*(2), 3046–9163.

Karima, N. A., Aisyah, A. N., Silla, H. V., Handoko, L. B., & Sani, R. R. (2024). Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit. *Jurnal Masyarakat Informatika*, *15*(1), 1–13.

Madarro-Capó, E. J., Legón-Pérez, C. M., Rojas, O., & Sosa-Gómez, G. (2021). Information theory based evaluation of the RC4 stream cipher outputs. *Entropy*, *23*(7), 896.

Maulana, R., & Simanjorang, R. M. (2021). Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4. *Jurnal Nasional Komputasi dan Teknologi Informasi*, *4*(6), 377–383.

Navintino, F. F., Fahreza, M. F., & Rilvani, E. (2025). Tinjauan Literatur: Perbandingan Sistem Keamanan Pada Aplikasi Android Dan Ios. *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer*, *4*(1), 22–28.

Ngemba, H. R., Ulhaq, M. N. D., Hendra, S., Azhar, R., Alamsyah, A., & Laila, R. (2024). Implementasi Algoritma Rc4 Pada Sistem Informasi Koperasi Virtual Bawaslu Provinsi Sulawesi Tengah Virtual Bawaslu. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *11*(1), 98–103.

Nurdiansyah, F. (2025). Penerapan Algoritma Caesar Cipher Pada Aplikasi Pengaman Pesan Berbasis Website. *Jurnal Teknologi Informasi*, *15*(2), 92–98. https://doi.org/10.36382/jti-tki.v15i2.530

Nurindahsari, F., & Zen, B. P. (2021). Analisis Statik Keamanan Aplikasi Video Streaming Berbasis Android Menggunakan Mobile Security Framework (Mobsf). *Cyber Security dan Forensik Digital*, *4*(2), 63–80.

Pradeka, D., Khaerunnisa, Z., Humaira, S. A., Billa, A. S., Murnawan, M., & Budiman, B. (2025). Digital Data Security Using a Combination of Base64 Encoding, Rail Fence Cipher, and GZIP Compression. *Journal of Computer Engineering, Electronics and Information Technology*, *4*(1), 51–60.

Pratiwi, R., Utami, L. C., & Sakti, R. B. (2022). Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher. *Bulletin of Information Technology (BIT)*, *3*(4), 367–373.

Purnamasari, S. D., & Panjaitan, F. (2020). Pengembangan Aplikasi E-Reporting Kerusakan Lampu Jalan Berbasis Mobile. *Jusikom: Jurnal Sistem Komputer Musirawas*, *5*(1), 59–69.

Purnomo, H. D., & Sembiring, I. (2022). Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks. *Journal of Information Technology*, *2*(1), 16–22.

Rahmawati, I., & Sari, D. P. (2024). Aplikasi Berbasis Android Menggunakan Flutter Framework untuk Keperluan Perizinan Tugas Keluar pada PT. XYZ. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *9*(2), 979–993.

Ramdani, F. C., Rahmatulloh, A., Shofa, R. N., Nomor, J. S., Tasikmalaya, J., & Barat, I. (2023). Implementasi JSON Web Token pada Authentication dengan Algoritma HMAC SHA-256 Implementation of JSON Web Token on Authentication with HMAC SHA-256 Algorithm. *Januari*, *12*(1), 2540–9719. http://sistemasi.ftik.unisi.ac.id

Ranto Siswanto, & Muawan Bisri. (2025). Penerapan Federated Learning dalam Keamanan Data Pengguna pada Aplikasi Mobile. *Jurnal Publikasi Teknik Informatika*, *4*(2), 01–09. https://doi.org/10.55606/jupti.v4i2.3990

Shiddiqramzy, H., & Sediyono, E. (2023). Perancangan Aplikasi Chat Realtime sebagai Media Bercerita Berbasis Android. *Jurnal Teknologi Informasi dan Komunikasi)*, *7*(2), 2023. https://doi.org/10.35870/jti

Siswidiyanto, S., Wijayanti, D., & Haryadi, E. (2020). Sistem Informasi Penyewaan Rumah Kontrakan Berbasis Web Dengan Menggunakan Metode Prototype. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi dan Komunikasi*, *15*(1), 16–23.

Soepeno, R. (2023). Wireshark: An Effective Tool for Network Analysis. *CYBV-Introd. Methods Netw. Anal*, 1–15.

Sopandi, A., Hannan, A. R., & Khotimah, H. (2024). Perancangan aplikasi mobile menggunakan framework Flutter pada sistem informasi akademik. *JIKA (Jurnal Informatika)*, *8*(3), 304–310.

Sugiyatno. (2023). Pengiriman Informasi Real Time Menggunakan Teknologi Database Firebase pada Aplikasi Mobile. *Bisnis dan Manajemen*, *21*(2).

Sulaksono, D. H., Prabiantissa, C. N., Yuliastuti, G. E., & Taqwa, A. R. (2021). Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android. *Prosiding Seminar Nasional Sains dan Teknologi Terapan*, *9*(1), 570–576.

Sumarto, M. A. (2023). Analisis Dan Perancangan Aplikasi Point Of Sale Berbasis Mobile Menggunakan Framework Flutter Dengan Metode Rapid Application Development (Rad). *Jurnal Studi Komunikasi Dan Media*, *27*(1), 17–34.

T P Sreedevi, & Dr V Harsha Shastri. (2025). Evolving Trends in Lightweight Cryptography for Secure IoT: Overcoming Challenges and Delivering Solutions. *International Research Journal on Advanced Engineering and Management (IRJAEM)*, *3*(04), 1428–1432. https://doi.org/10.47392/irjaem.2025.0232

Wardhana, F. K., Kurniawan, A., Seto, B. R., & Saputro, I. A. (2023). Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 Dan AES. *Prosiding Seminar Nasional Amikom Surakarta*, *1*, 124–134.

Zhang, L., & Wang, L. (2024). A hybrid encryption approach for efficient and secure data transmission in IoT devices. *Journal of Engineering and Applied Science*, *71*(1), 138.

Zinkus, M., Jois, T. M., & Green, M. (2021). SoK: Cryptographic confidentiality of data on mobile devices. *arXiv preprint arXiv:2109.11007*.