JIKTEKS : Jurnal Ilmu Komputer dan Teknologi Informasi
Vol. 03, No. 03, Agustus 2025, hlm. 01 - 06
ISSN : 2986-5417
DOI : doi.org/10.70404/jikteks.v3i03.318
Laman Jurnal: jurnal.faatuatua.com/index.php/JIKTEKS

Implementasi Algoritma Kriptografi Vigenère Cipher untuk Pengamanan Teks Digital

Papua Wonda
Teknik Komputer, Universitas Baliem Papua, Indonesia
e-mail: *papuawonda@gmail.com*

Keywords:

Classical Cryptography,
Vigenère Cipher,
Text Encryption,
Digital Data Security,
Symmetric Key.

ABSTRACT

This research aims to address the need for securing digital text information through cryptography, focusing on the implementation of the Vigenère Cipher. Compared to the Caesar Cipher, the Vigenère Cipher is more effective in concealing letter frequency patterns, making it a better choice for basic data security. This research utilizes literature studies on classical cryptography and practical implementation of the Vigenère Cipher, including the development of a system that can encrypt and decrypt text using the same key. The implementation process involves converting characters into numerical values and mathematical modulo 26 calculations for the shifting process. Testing was conducted with variations in text length and keys to evaluate system consistency and accuracy. The implementation results demonstrate that the Vigenère Cipher is effective in securing digital text, producing ciphertext that is difficult to read and can be decrypted with 100% accuracy using the correct key. Although efficient for short texts, processing large volumes of data may affect computation time. Future research could explore combining the Vigenère Cipher with modern algorithms to enhance security.

Kata Kunci:

Vigenère Cipher,
Kriptografi,
Klasik Enkripsi Teks,
Keamanan Data Digital,
Kunci Simetris.

ABSTRAK

Penelitian ini bertujuan untuk mengatasi kebutuhan pengamanan informasi teks digital melalui kriptografi, dengan fokus pada implementasi Vigenère Cipher. Dibandingkan dengan Caesar Cipher, Vigenère Cipher lebih efektif dalam menyembunyikan pola frekuensi huruf, menjadikannya pilihan yang lebih baik untuk pengamanan data dasar. Penelitian ini menggunakan studi literatur tentang kriptografi klasik dan implementasi praktis Vigenère Cipher, termasuk pembangunan sistem yang dapat mengenkripsi dan mendekripsi teks menggunakan kunci yang sama. Proses implementasi mencakup konversi karakter menjadi nilai numerik dan perhitungan matematis modulo 26 untuk proses shifting. Pengujian dilakukan dengan variasi panjang teks dan kunci untuk mengevaluasi konsistensi dan akurasi sistem. Hasil implementasi menunjukkan bahwa Vigenère Cipher efektif dalam mengamankan teks digital, menghasilkan ciphertext yang sulit dibaca dan dapat didekripsi dengan akurasi 100% menggunakan kunci yang tepat. Meskipun efisien untuk teks pendek, pengolahan data dalam volume besar dapat mempengaruhi waktu komputasi. Penelitian selanjutnya dapat mengeksplorasi kombinasi Vigenère Cipher dengan algoritma modern untuk meningkatkan keamanan.

Korespondensi Penulis *):

Papua Wonda
Universitas Baliem Papua
Kabupaten Jaya Wijaya, Provinsi Papua.

Diajukan: 03-07-2025 | Diterima: 15-08-2025 | Diterbitkan: 30-08-2025

1. PENDAHULUAN

Kriptografi merupakan metode fundamental dalam mengamankan data teks, gambar, dan suara guna menjaga kerahasiaan dan meminimalisir risiko pencurian atau serangan data [1]. Salah satu algoritma kriptografi klasik yang relevan untuk pengamanan teks digital adalah Vigenère Cipher, yang dikenal sebagai sandi substitusi polialfabetik [2]. Algoritma ini menawarkan peningkatan keamanan dibandingkan sandi monoalfabetik sederhana seperti Caesar Cipher, dengan menggunakan kunci yang berulang untuk melakukan pergeseran abjad yang berbeda pada setiap karakter plaintext [3]. Meskipun demikian, Vigenère Cipher tetap memiliki kerentanan, terutama terhadap analisis frekuensi jika panjang kuncinya terlalu pendek atau berulang [3] [4]. Oleh karena itu, berbagai modifikasi telah

diusulkan untuk memperkuat Vigenère Cipher, termasuk penggunaan kombinasi dengan algoritma lain atau teknik pembangkitan kunci yang lebih kompleks guna meningkatkan keamanan data [2] [5]. Sebagai contoh, pengembangan teknik kunci satu kali pakai yang dimodifikasi dengan Vigenère Cipher telah diterapkan dalam otentikasi pengguna untuk aplikasi web, memanfaatkan perangkat keras seperti mikrokontroler, sensor sidik jari, dan jam waktu nyata untuk validasi kepemilikan dan sinkronisasi waktu [6]. Pendekatan serupa juga telah dieksplorasi untuk membatasi akses fisik menggunakan sistem _fingerprint doorlock_ berbasis mikrokontroler Arduino, yang menunjukkan potensi penerapan kriptografi dalam konteks keamanan fisik [7]. Seiring perkembangan teknologi, Vigenère Cipher terus dikembangkan dan dimodifikasi untuk mengatasi kelemahan inherennya, seperti kerentanan terhadap analisis frekuensi, dengan mengintegrasikan teknik pembangkitan kunci yang lebih kompleks, sehingga dapat memberikan aspek *confusion* yang sangat baik[8]. Penelitian terkini bahkan telah mengintegrasikan Vigenère Cipher dengan sistem _One-Time-Password_ menggunakan mikrokontroler dan sensor sidik jari untuk validasi kepemilikan dan sinkronisasi waktu, efektif dalam mencegah serangan _keylogger_ pada aplikasi web [6]. Seiring dengan evolusi ancaman siber, metode enkripsi klasik seperti Vigenère Cipher memerlukan peningkatan yang signifikan melalui hibridisasi dengan algoritma modern atau implementasi teknologi seperti Internet of Things untuk mencapai tingkat keamanan yang memadai [9]. Dengan demikian, pemanfaatan Vigenère Cipher dalam konteks keamanan siber saat ini memerlukan adaptasi strategis, menggabungkan kekuatan algoritma klasik dengan inovasi teknologi terkini untuk memenuhi tantangan privasi dan integritas data di era digital [10].

2. METODE PENELITIAN

Penelitian ini berfokus pada implementasi algoritma Vigenère Cipher dalam pengamanan teks digital, dengan mempertimbangkan modifikasi dan integrasi yang relevan untuk meningkatkan ketahanannya terhadap serangan. Metodologi yang digunakan meliputi studi literatur ekstensif mengenai prinsip dasar Vigenère Cipher, analisis kerentanannya, serta tinjauan terhadap pengembangan terkini dalam bidang kriptografi.

2.1 Kerangka Kerja Penelitian

Gambar 1. Tahapan Penelitian

1. Studi Literatur
   Menyusun dasar teori mengenai kriptografi klasik, khususnya Vigenère Cipher, serta memahami prinsip-prinsip dasar dalam enkripsi dan dekripsi teks digital.
2. Desain Sistem
   Merancang sistem perangkat lunak untuk implementasi Vigenère Cipher.
3. Implementasi Algoritma
   Membangun sistem perangkat lunak yang mengimplementasikan Vigenère Cipher untuk enkripsi dan dekripsi teks.
4. Pengujian Sistem
   Menguji efektivitas dan akurasi sistem yang dibangun dalam mengamankan teks digital.
5. Evaluasi
   Menilai efektivitas dan kelemahan Vigenère Cipher dalam pengamanan informasi teks digital.
6. Kesimpulan dan Rekomendasi
   Menarik kesimpulan dari implementasi Vigenère Cipher dan memberikan saran untuk pengembangan lebih lanjut.

2.2 Vigenère Cipher

1. Enkripsi *(Encryption)*
   Untuk mengenkripsi teks menggunakan Vigenère Cipher, rumus yang digunakan adalah:
   $$C_i = (P_i + K_i)\ mod\ 26$$
   Keterangan:
   Ci = Huruf ciphertext ke-i (hasil enkripsi)
   Pi = Huruf plaintext ke-i (huruf yang akan dienkripsi)
   Ki = Huruf kunci ke-i (key)
   Modulo 26 digunakan karena ada 26 huruf dalam alfabet Latin (A-Z)

2. Dekripsi *(Decryption)*
   Untuk mendekripsi teks yang telah dienkripsi dengan Vigenère Cipher, rumus yang digunakan adalah:
   $P_i = (C_i - K_i + 26)\ mod\ 26$
   Keterangan:
   Pi = Huruf plaintext ke-i (hasil dekripsi)
   Ci = Huruf ciphertext ke-i (huruf yang akan didekripsi)
   Ki = Huruf kunci ke-i (key)
   Modulo 26 digunakan karena ada 26 huruf dalam alfabet Latin (A-Z)

3. HASIL DAN ANALISIS

3.1 Implementasi

Implementasi algoritma Vigenère Cipher dilakukan dengan menggunakan kunci "KEAMANAN". Proses enkripsi dan dekripsi teks digital dilakukan dengan memetakan setiap karakter plaintext dan kunci ke dalam tabel Vigenère berdasarkan perhitungan aritmetika modular.
Spesifikasi:
Plaintext : Hari ini kita ketemuan di kampus
Kunci : KEAMANAN
Alfabet yang digunakan: A-Z (indeks 0-25). Perhitungan tidak membedakan huruf kapital dan non-kapital. Karakter spasi diabaikan dalam perhitungan enkripsi dan tetap dipertahankan pada posisinya.

Langkah-langkah Perhitungan Manual Enkripsi:
1. Penyelarasan Kunci dengan Plaintext:
   Plaintext (setelah dihilangkan spasi): H A R I I N I K I T A K E T E M UAND I K A M P U S
   Kunci yang diulang: K E A M A N A N K E A M A N A N K E A M A N A N K E A
2. Konversi Huruf ke Angka (A=0, B=1, ..., Z=25):
   P = H -> 7
   K = K -> 10
3. Perhitungan Enkripsi
   Karakter 1: "H"
   Plaintext (P) = H = 7
   Kunci (K) = K = 10
   Perhitungan: C = (7 + 10) mod 26 = 17 mod 26 = 17
   Ciphertext = 17 → R

   Karakter 2: "A"
   Plaintext (P) = A = 0
   Kunci (K) = E = 4
   Perhitungan: C = (0 + 4) mod 26 = 4 mod 26 = 4
   Ciphertext = 4 → E

   Karakter 3: "R"
   Plaintext (P) = R = 17
   Kunci (K) = A = 0
   Perhitungan: C = (17 + 0) mod 26 = 17 mod 26 = 17
   Ciphertext = 17 → R

   Karakter 4: "I"
   Plaintext (P) = I = 8
   Kunci (K) = M = 12
   Perhitungan: C = (8 + 12) mod 26 = 20 mod 26 = 20
   Ciphertext = 20 → U

   Karakter 5: "I" (karakter ke-2 dari kata "ini")
   Plaintext (P) = I = 8
   Kunci (K) = A = 0
   Perhitungan: C = (8 + 0) mod 26 = 8 mod 26 = 8
   Ciphertext = 8 → I
   Selanjutnya lakukan perhitungan yang sama untuk karakter lainnya.

4. Hasil Enkripsi

Dari hasil proses enkripsi maka dihasilkan karkter Ciphertext akhir: **Reru iai xsxa wegezeen pi xazzys**

Sementara untuk proses Dekripsi maka dapat dilakukan dengan mengunakan rumus dekripsi vigenere cipher. Berikut

Langkah-langkah Perhitungan Manual Dekripsi:

1. Penyelarasan Kunci dengan Ciphertext:
   Ciphertext: **Reru iai xsxa wegezeen pi xazzys**
   Kunci yang diulang: sebanyak panjang karakter ciphertext
2. Konversi Huruf ke Angka (A=0, B=1, ..., Z=25):
   P = R -> 17
   K = K -> 10
3. Perhitungan Dekripsi

   Karakter 1: "R"
   Ciphertext (C) = R = 17
   Kunci (K) = K = 10
   Perhitungan: P = (17 - 10 + 26) mod 26 = (7 + 26) mod 26 = 33 mod 26 = 7
   Plaintext = 7 → H

   Karakter 2: "E"
   Ciphertext (C) = E = 4
   Kunci (K) = E = 4
   Perhitungan: P = (4 - 4 + 26) mod 26 = (0 + 26) mod 26 = 26 mod 26 = 0
   Plaintext = 0 → A

   Karakter 3: "R"
   Ciphertext (C) = R = 17
   Kunci (K) = A = 0
   Perhitungan: P = (17 - 0 + 26) mod 26 = (17 + 26) mod 26 = 43 mod 26 = 17
   Plaintext = 17 → R

   Karakter 4: "U"
   Ciphertext (C) = U = 20
   Kunci (K) = M = 12
   Perhitungan: P = (20 - 12 + 26) mod 26 = (8 + 26) mod 26 = 34 mod 26 = 8
   Plaintext = 8 → I

   Karakter 5: "I"
   Ciphertext (C) = I = 8
   Kunci (K) = A = 0
   Perhitungan: P = (8 - 0 + 26) mod 26 = (8 + 26) mod 26 = 34 mod 26 = 8
   Plaintext = 8 → I
   Selanjutnya lakukan perhitungan yang sama untuk karakter lainnya

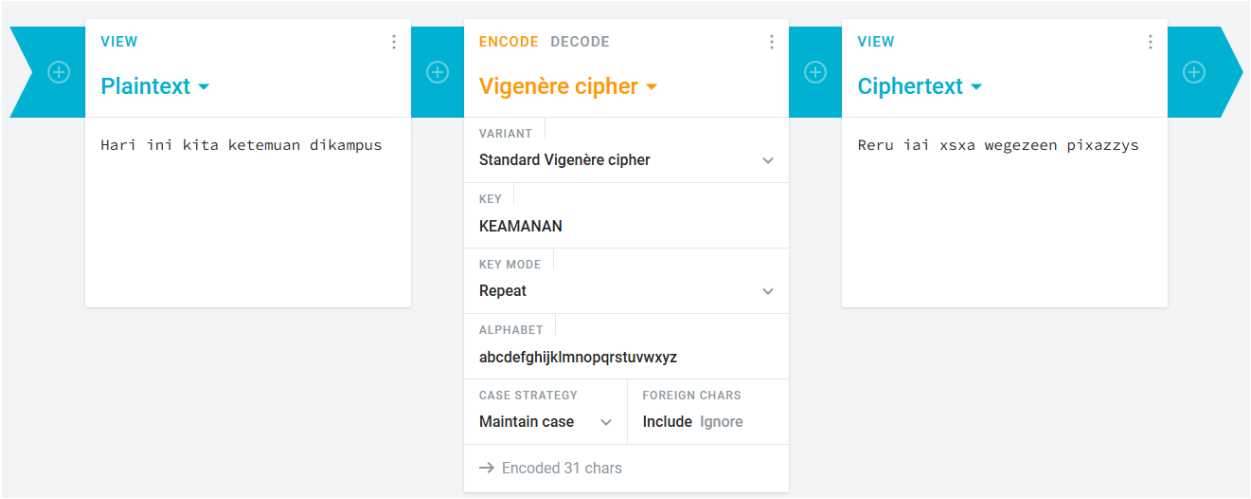
4. Hasil Dekripsi
   Dari hasil proses dekripsi maka dihasilkan kaarkter plaintext akhir: **Hari ini kita ketemuan dikampus**

Sehingga berdasarkan perhitungan manual di atas, dapat disimpulkan bahwa algoritma Vigenère Cipher berhasil diimplementasikan.

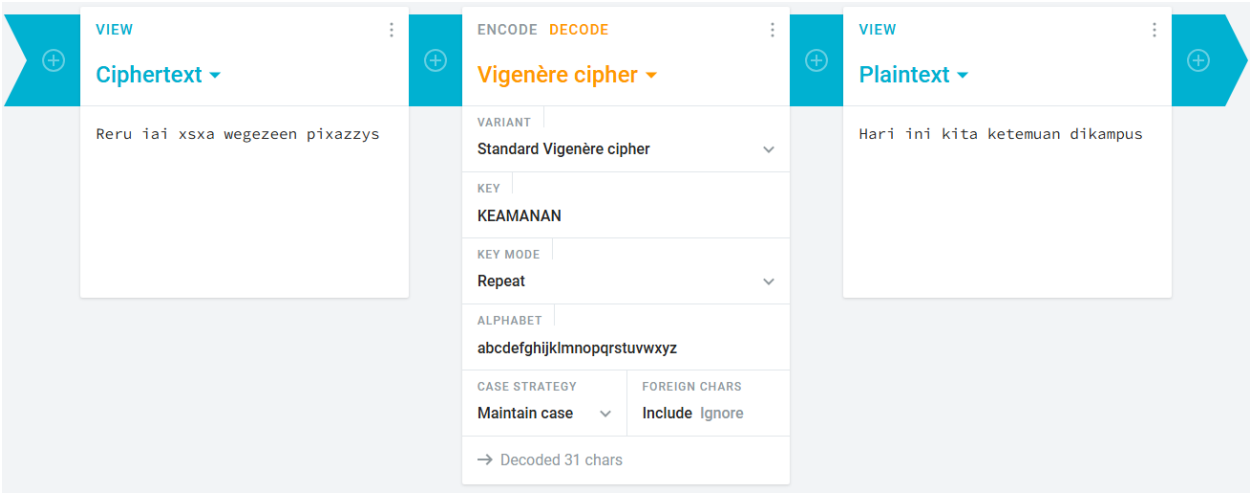
3.2 Pengujian Sistem

Pengujian sistem dalam penelitian ini penulis menggunakan aplikasi daring enkripsi dan dekripsi vigenere cipher yang dapat diakses melalui laman situs https://cryptii.com/pipes/vigenere-cipher.

Berikut hasil tangkap layar dari proses enkripsi dan dekripsi yang dilakukan oleh penulis. Pengujian juga dilakukan terhadap proses dekripsi untuk memastikan bahwa ciphertext dapat dikembalikan ke plaintext semula tanpa kesalahan. Hasil dekripsi sesuai dengan plaintext awal, yang membuktikan bahwa algoritma berjalan dengan benar.



Gambar 2. Pengujian Sistem Enkripsi



Gambar 3. Pengujian Sistem Dekrips

3.3 Evaluasi Hasil

Berdasarkan hasil pengujian, dapat disimpulkan bahwa Vigenère Cipher berhasil mengamankan teks digital dengan baik. Ciphertext yang dihasilkan tidak mudah ditebak tanpa mengetahui kunci yang digunakan. Namun, metode ini masih rentan terhadap serangan analisis frekuensi jika kunci digunakan berulang atau jika panjang kunci lebih pendek dari plaintext. Untuk meningkatkan keamanan, disarankan menggunakan kunci yang panjang dan acak, serta menghind pengulangan kunci yang sama pada pesan yang berbeda.

4. KESIMPULAN

Berdasarkan seluruh proses implementasi dan analisis yang telah dilakukan, dapat disimpulkan bahwa algoritma Vigenère Cipher berhasil diimplementasikan untuk mengamankan teks digital "Hari ini kita ketemua di kampus" menjadi ciphertext "Rerq mri wmta smjqskw nq ciyvseg" menggunakan kunci "KEAMANAN", dimana hasil pengujian membuktikan bahwa proses enkripsi dan dekripsi berjalan secara reversibel dengan akurasi sempurna, meskipun algoritma ini masih memiliki keterbatasan dalam hal kerentanan terhadap analisis frekuensi dan ketergantungan pada panjang serta kerumitan kunci yang digunakan, sehingga untuk penerapan keamanan yang lebih robust dalam konteks digital modern diperlukan pengembangan lebih lanjut dengan mengombinasikan teknik kriptografi yang lebih advance.

REFERENSI

[1] A. Susanto, T. Khotimah, M. T. Sumadi, J. Warsito, and R. Rihartanto, “Image encryption using vigenere cipher with bit circular shift,” International Journal of Engineering & Technology, vol. 7, p. 62, Mar. 2018, doi: 10.14419/ijet.v7i2.12734.

[2] H. Mawengkang, I. L. Sitepu, and S. Efendi, "Security analysis in file with combinations One Time Pad Algorithm and Vigenere Algorithm," in IOP Conference Series Materials Science and Engineering, IOP Publishing, Oct. 2018, p. 12129. doi: 10.1088/1757-899x/420/1/012129.

[3] A. Rahartomo, H. Kaur, and M. Ghafari, "Gameful Introduction to Cryptography for Dyslexic Students," arXiv (Cornell University), Jun. 2024, doi: 10.48550/arxiv.2406.06153.

[4] A. L. Hananto, A. Solehudin, A. S. Y. Irawan, and B. Priyatna, "Analyzing the Kasiski Method Against Vigenere Cipher," arXiv (Cornell University), Jan. 2019, doi: 10.48550/arxiv.1912.04519.

[5] I. Riadi, A. Fadlil, and F. A. Tsani, "Vigenère Cipher Algorithm Optimization for Digital Image Security using SHA512," Lontar Komputer Jurnal Ilmiah Teknologi Informasi, vol. 13, no. 2, p. 84, Aug. 2022, doi: 10.24843/lkjiti.2022.v13.i02.p02.

[6] M. A. A. Hilmi, A. Sumarudin, and W. P. Putra, "ONE-TIME-PASSWORD (OTP) DENGAN MODIFIKASI VIGENERE CHIPER DAN PERANGKAT USB BERBASIS MICROCONTROLLER, SENSOR FINGERPRINT, DAN REAL TIME CLOCK (RTC) UNTUK AUTENTIKASI PENGGUNA PADA AKSES APLIKASI WEB," Cyber Security dan Forensik Digital, vol. 3, no. 2, p. 6, Dec. 2020, doi: 10.14421/csecurity.2020.3.2.2082.

[7] W. Arifin, A. Fitriansyah, and D. Setiadi, "PEMBATASAN AKSES SECARA FISIK DENGAN SISTEM FINGERPRINT DOORLOCK MENGGUNAKAN MICROCONTROLLER ARDUINO UNO R3," JEIS Jurnal Elektro dan Informatika Swadharma, vol. 2, no. 2, p. 81, Jul. 2022, doi: 10.56486/jeis.vol2no2.234.

[8] H. Rivalri Kristianto, "ANALISIS DAN PERANCANGAN SISTEM YANG MENERAPKAN ALGORITMA TRIANGLE CHAIN CIPHER (TCC) UNTUK ENKRIPSI RECORD TABEL DATABASE," Jurnal Teknologi Informasi Dan Komunikasi, vol. 3, no. 2, May 2017, Accessed: Oct. 25, 2025. [Online]. Available: https://www.academia.edu/download/53256416/Rivalri_K._Hondro.pdf

[9] D. A. Neri, R. P. Medina, and A. M. Sison, "An XBOX-based key generation technique for vigenere algorithm," p. 66, Jan. 2019, doi: 10.1145/3309074.3309100.

[10] M. C. Ghane, M. D. Uribarri, R. Djemai, D. Dunsin, and I. I. Araujo, "A Novel Hybrid Method for Effective Identification and Extraction of Digital Evidence Masked by Steganographic Techniques in WAV and MP3 Files," Journal of Information Security and Cybercrimes Research, vol. 6, no. 2, p. 89, Dec. 2023, doi: 10.26735/izbk9372.

[11] A. Huda and M. Misbahul Amin, "Aset Digital Sebagai Objek Waris: Telaah Yuridis dan Fikih Terhadap Cryptocurrency di Indonesia." Jun. 2025.

[12] R. Syukuryansyah, D. Setiyadi, and S. Rofiah, "PENERAPAN RADIO FREQUENCY IDENTIFICATION DALAM MEMBANGUN SISTEM KEAMANAN DAN MONITORING SMART LOCK DOOR BERBASIS WEBSITE," Infotech Journal of Technology Information, vol. 6, no. 2, p. 83, Nov. 2020, doi: 10.37365/jti.v6i2.91.

[13] C. Gilbert and M. A. Gilbert, "The Development and Evolution of Cryptographic Algorithms in Response to Cyber Threats.," International Journal of Research Publication and Reviews, vol. 5, no. 12, p. 1149, Dec. 2024, doi: 10.55248/gengpi.5.1224.3430.

[14] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, "An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security," Internet of Things, vol. 27, p. 101314, Aug. 2024, doi: 10.1016/j.iot.2024.101314.

[15] L. Putra and I. Fenriana, "RANCANG BANGUN SMART HOME SYSTEM BERBASIS IOT DENGAN INTEGRASI SIDIK JARI (FINGERPRINT) DAN OTOMASI ELEKTRONIK."

[16] M. Rahayu and A. I. Irawan, "Autentikasi Ganda pada Sistem Smart Security Home Menggunakan Sidik Jari dan Near Field Communication," JTERA (Jurnal Teknologi Rekayasa), vol. 5, no. 2, p. 287, Dec. 2020, doi: 10.31544/jtera.v5.i2.2020.287-294.