

## **Integrasi Seni Kuno dan Tantangan Enkripsi Modern melalui Kajian Ulang Teknik Kriptanalisis Al-Kindi**

**Anatansyah Ayomi Anandari, Rudy Agus Gemilang Gultom**  
Program Studi Teknologi Penginderaan, Fakultas Sains dan Teknologi  
Pertahanan, Universitas Pertahanan Republik Indonesia  
Email: anatanayomiii@gmail.com, rudygultom@idu.ac.id

### **Abstract**

*This study aims to review the cryptanalysis techniques introduced by Al-Kindi, an ancient cryptographic figure, by relating them to the modern encryption challenges faced today. The method used involves an analysis of the literature on Al-Kindi's works which are relevant in cryptanalysis, such as "Risalah al-Mu'atabarah". In addition, the ancient cryptanalysis techniques introduced by Al-Kindi are also analyzed in the context of complex modern encryption challenges. The results of this study indicate that the cryptographic principles proposed by Al-Kindi, such as the substitution method, the transposition method, and the need for a strong secret key, still have relevance in overcoming modern encryption challenges. The method of substitution and transposition introduced by Al-Kindi can be adapted in letter frequency analysis and structural analysis to decode complex codes. The principle of needing a strong secret key also remains important in protecting data and communications in the modern digital era. The cryptographic principles introduced by Al-Kindi can be applied in overcoming the complexity of the current encryption system. This research provides new insights into how to apply ancient cryptographic principles to crack complex codes and improve information security in the ever-evolving digital age.*

**Keywords:** *Al-Kindi, Cryptanalysis, Cryptography, Encryption, Information Security*

### **Pendahuluan**

Perkembangan teknologi modern telah membawa dampak signifikan dalam bidang enkripsi dan keamanan informasi<sup>1</sup>. Dalam beberapa dekade terakhir, kita telah menyaksikan kemajuan pesat dalam pengembangan sistem enkripsi yang lebih kuat dan kompleks. Namun, bersamaan dengan itu, tantangan dalam memecahkan kode-kode yang semakin kompleks juga menjadi semakin sulit<sup>2</sup>. Salah satu tantangan utama yang dihadapi dalam memecahkan kode-kode kompleks adalah meningkatnya kekuatan komputasi. Seiring dengan perkembangan teknologi, komputer-komputer modern memiliki kemampuan pemrosesan yang jauh lebih cepat dan lebih kuat dibandingkan dengan komputer-komputer sebelumnya<sup>3</sup>. Hal ini juga berarti bahwa proses kriptanalisis yang sebelumnya memakan waktu

---

<sup>1</sup> Aldi Renaldy et al., "Peran Sistem Informasi Dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan," *Jurnal Ilmu Multidisiplin* 2, no. 1 (2023): 15–22.

<sup>2</sup> Yudi Wiharto and Ari Irawan, "Enkripsi Data Menggunakan AES 256," *Jurnal Kilat* 7, no. 2 (2018): 91–99.

<sup>3</sup> Albert Ginting, R. Rizal Isnanto, and Ike Pertiwi Windasari, "Implementasi Algoritma Kriptografi RSA Untuk Enkripsi Dan Dekripsi Email," *Jurnal Teknologi Dan Sistem Komputer* 3, no. 2 (2015): 253–58, <https://jtsiskom.undip.ac.id/article/view/12009>.

berbulan-bulan atau bahkan bertahun-tahun, sekarang dapat diselesaikan dalam hitungan jam atau menit.

Selain itu, adanya teknik-teknik enkripsi yang lebih canggih juga menjadi tantangan tersendiri. Misalnya, algoritma enkripsi kunci publik seperti RSA dan *Elliptic Curve Cryptography* (ECC) telah menjadi standar industri dalam mengamankan komunikasi digital<sup>4</sup>. Algoritma-algoritma ini didasarkan pada matematika yang kompleks dan sulit untuk dipecahkan secara langsung. Oleh karena itu, memecahkan kode-kode yang menggunakan enkripsi yang kuat seperti itu membutuhkan pendekatan yang lebih terfokus dan mungkin melibatkan serangan terhadap kelemahan-kelemahan yang mungkin ada dalam implementasi spesifik algoritma tersebut<sup>5</sup>. Selain kekuatan komputasi dan kompleksitas algoritma, faktor lain yang memperumit kriptanalisis adalah jumlah data yang perlu dianalisis. Dalam era digital saat ini, jumlah data yang dihasilkan dan ditransmisikan secara online sangatlah besar. Menganalisis dan memecahkan kode-kode dalam jumlah data yang sedemikian besar menjadi sangat menantang dan memerlukan pendekatan analisis yang efisien dan skalabel<sup>6</sup>.

Selanjutnya, perkembangan teknologi lain seperti komputasi awan dan *Internet of Things* (IoT) juga memperkenalkan tantangan baru dalam hal keamanan dan enkripsi. Komputasi awan memungkinkan penyimpanan dan pemrosesan data yang besar secara eksternal, yang berarti informasi sensitif dapat diakses oleh pihak-pihak yang tidak berwenang jika tidak dienkripsi dengan benar<sup>7</sup>. Sementara itu, IoT membawa miliaran perangkat terhubung yang saling berkomunikasi, dan memerlukan sistem enkripsi yang aman dan efisien untuk melindungi data yang dikirimkan melalui jaringan yang rentan. Dalam menghadapi tantangan ini, para ahli kriptografi terus mengembangkan teknik-teknik baru untuk mengamankan informasi dan memecahkan kode-kode yang kompleks<sup>8</sup>. Salah satu pendekatan yang digunakan adalah kombinasi dari *Artificial Intelligence* (AI) dan komputasi berkecepatan tinggi untuk meningkatkan efisiensi proses kriptanalisis. Teknik-teknik ini melibatkan penggunaan kecerdasan buatan untuk mengidentifikasi pola-pola dan kelemahan dalam kode-kode yang dienkripsi, serta penggunaan sumber

---

<sup>4</sup> Dindayal Mahto and Dilip Kumar Yadav, "RSA and ECC, A Comparative Analysis.Pdf," *International Journal of Applied Engineering Research* 12, no. 19 (2017): 9053–61.

<sup>5</sup> S. Suyanto, "Keamanan Database Menggunakan Metode Enkripsi," *Jurnal Ilmiah Matrik*, no. 12 (2012): 137–50.

<sup>6</sup> Raodia Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)," *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019): 39, <https://doi.org/10.24252/jurisprudentie.v6i2.11399>.

<sup>7</sup> Ricky Maulana Fajrin et al., "Keamanan Data Pada Cloud Computing," *Seminar Nasional Teknologi Informasi, Komunikasi Dan Manajemen Palembang-Indonesia* 23 (2014).

<sup>8</sup> Wiharto and Irawan, "Enkripsi Data Menggunakan AES 256."

daya komputasi yang tinggi untuk mengurangi waktu yang dibutuhkan dalam proses tersebut<sup>9</sup>.

Pendekatan lain yang digunakan adalah kolaborasi dan pertukaran pengetahuan antara para peneliti dan profesional dalam bidang kriptografi. Dengan berbagi pengetahuan dan pengalaman, komunitas kriptografi dapat secara kolektif menghadapi tantangan enkripsi modern dengan cara yang lebih efektif<sup>10</sup>. Konferensi, seminar, dan forum online menjadi platform penting bagi para ahli untuk berinteraksi, berdiskusi, dan memperbarui teknik-teknik kriptanalisis mereka. Perkembangan teknologi modern telah membawa perubahan besar dalam bidang enkripsi dan kriptanalisis. Tantangan yang dihadapi dalam memecahkan kode-kode kompleks semakin rumit dengan kekuatan komputasi yang semakin kuat, kompleksitas algoritma, volume data yang besar, dan perkembangan teknologi lainnya. Namun, dengan pendekatan yang inovatif, kolaborasi yang erat, dan pengembangan teknik-teknik baru, kita dapat terus mengatasi tantangan ini dan meningkatkan keamanan informasi dalam era digital yang terus berkembang.

Al-Kindi, yang dikenal juga sebagai Abu Yusuf Ya'qub ibn Ishaq al-Kindi, adalah seorang cendekiawan Muslim yang hidup pada abad ke-9 Masehi. Ia dikenal sebagai salah satu tokoh kriptografi kuno yang memainkan peran penting dalam pengembangan teknik kriptanalisis. Al-Kindi dilahirkan di wilayah Kufah, Irak, pada sekitar tahun 801 Masehi, dan ia menunjukkan minat yang besar dalam bidang matematika, fisika, dan filsafat. Salah satu karya penting Al-Kindi dalam bidang kriptografi adalah "*Risalah al-Mu'atabarah*" atau "*The Treatise on Cryptanalysis*". Dalam risalah ini, ia menyajikan metode-metode kriptanalisis untuk memecahkan berbagai jenis sandi dan sistem enkripsi yang digunakan pada masanya. Al-Kindi berpendapat bahwa metode ilmiah dan analisis logis dapat digunakan untuk memecahkan kode-kode rahasia<sup>11</sup>.

Al-Kindi mengembangkan prinsip-prinsip kriptografi yang penting, termasuk metode substitusi dan transposisi. Metode substitusi melibatkan penggantian huruf-huruf dalam teks terenkripsi dengan huruf-huruf lain berdasarkan aturan tertentu. Metode transposisi, di sisi lain, melibatkan perubahan posisi huruf-huruf dalam teks terenkripsi. Al-Kindi juga mengeksplorasi konsep probabilitas dalam kriptanalisis, yaitu memanfaatkan frekuensi kemunculan huruf-huruf atau pola-pola tertentu

---

<sup>9</sup> Elena C. Laskari et al., *Cryptography and Cryptanalysis through Computational Intelligence, Studies in Computational Intelligence*, vol. 57, 2007, [https://doi.org/10.1007/978-3-540-71078-3\\_1](https://doi.org/10.1007/978-3-540-71078-3_1).

<sup>10</sup> Ismi Kaniawulan, M Rafi Muttaqin, and Dhiya Ulhaq, "Sistem Manajemen Pengetahuan Forum Diskusi Dosen Knowledge Management System of Lecturer Discussion Forum," *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIK)* 7, no. 1 (2020): 51–58, <https://doi.org/10.25126/jtiik.202071258>.

<sup>11</sup> Noor R. Al-kazaz, *Compression-Based Methods for the Automatic Cryptanalysis of Classical Ciphers College of Environmental Sciences and Engineering Compression-Based Methods for the Automatic Cryptanalysis of Classical* Noor R. Al-Kazaz (Bangor University, 2020).

dalam bahasa yang digunakan. Selain "*Risalah al-Mu'atabarah*", Al-Kindi juga menghasilkan karya lain yang berjudul "*Ilmu Tentang Dekripsi Sandi Rahasia*". Karya ini membahas prinsip-prinsip dasar dalam kriptografi, termasuk penggunaan kunci rahasia dan teknik-teknik untuk mengamankan komunikasi. Al-Kindi menyadari pentingnya menjaga kerahasiaan kunci dalam proses enkripsi dan dekripsi, dan ia mengembangkan metode-metode untuk menghasilkan kunci yang kuat dan sulit dipecahkan oleh pihak yang tidak berwenang.

Meskipun Al-Kindi hidup pada zaman kuno, kontribusinya dalam kriptanalisis memiliki relevansi yang kuat dengan tantangan enkripsi modern. Prinsip-prinsip yang diajukan oleh Al-Kindi, seperti metode substitusi dan transposisi, masih digunakan dalam teknik-teknik kriptografi modern. Selain itu, konsep probabilitas yang diperkenalkan oleh Al-Kindi juga penting dalam analisis statistik dalam kriptanalisis modern. Tujuan dari penelitian ini adalah untuk menjembatani kesenjangan antara seni kuno dalam kriptanalisis dan tantangan enkripsi modern yang dihadapi dalam era digital saat ini. Melalui kajian ulang terhadap teknik kriptanalisis Al-Kindi, dapat diharapkan untuk menghubungkan seni kuno kriptanalisis dengan tantangan enkripsi modern. Penelitian ini dapat mengungkapkan potensi penggunaan prinsip-prinsip Al-Kindi dalam mengatasi kelemahan-kelemahan pada enkripsi modern dan memberikan wawasan baru tentang pendekatan kriptanalisis yang dapat diterapkan pada sistem-sistem keamanan saat ini. Dengan mempelajari warisan kriptografi kuno, diharapkan dapat memperluas pengetahuan tentang prinsip-prinsip dasar kriptografi dan meningkatkan pemahaman tentang kompleksitas tantangan enkripsi yang dihadapi saat ini.

### **Metode Penelitian**

Metode penelitian yang digunakan dalam kajian ulang ini mencakup beberapa tahapan untuk memperoleh pemahaman yang komprehensif tentang teknik kriptanalisis Al-Kindi dan bagaimana prinsip-prinsipnya dapat diterapkan pada tantangan enkripsi modern. Tahapan-tahapan tersebut meliputi studi literatur, analisis teknik kriptanalisis Al-Kindi, identifikasi relevansi dengan tantangan enkripsi modern, dan penyusunan konsep baru. Penelitian ini akan dimulai dengan melakukan studi literatur yang komprehensif tentang karya-karya Al-Kindi yang relevan dalam kriptanalisis. Langkah ini bertujuan untuk memahami secara mendalam prinsip-prinsip kriptografi yang diperkenalkan oleh Al-Kindi dan teknik-teknik kriptanalisis yang digunakan<sup>12</sup>. Studi literatur akan melibatkan pengumpulan dan analisis terhadap karya-karya Al-Kindi yang mencakup "*Risalah al-Mu'atabarah*" dan "*Ilmu Tentang Dekripsi Sandi Rahasia*". Selanjutnya, tahap

---

<sup>12</sup> Budi Sulistyono, *Kriptanalisis Cipher Blok Berdasarkan Permainan Kaotik*, vol. 33204013 (Bandung: INSTITUT TEKNOLOGI BANDUNG, 2009).

analisis teknik kriptanalisis Al-Kindi akan dilakukan dengan fokus pada teknik-teknik yang diperkenalkan oleh Al-Kindi, seperti metode substitusi dan metode transposisi. Analisis ini akan mencakup pemahaman mendalam tentang prinsip-prinsip kriptografi yang ada dalam setiap teknik serta langkah-langkah yang dilakukan dalam menerapkan teknik-teknik ini dalam kriptanalisis.

Setelah memahami teknik-teknik kriptanalisis Al-Kindi, penelitian ini akan melanjutkan dengan analisis tentang bagaimana prinsip-prinsip ini dapat diterapkan pada tantangan enkripsi modern yang dihadapi saat ini. Analisis ini akan mempertimbangkan kompleksitas algoritma, perkembangan kekuatan komputasi, dan penggunaan teknologi dalam sistem enkripsi modern. Hal ini bertujuan untuk mengidentifikasi relevansi teknik-teknik kriptanalisis Al-Kindi dengan tantangan enkripsi modern yang kompleks. Penelitian ini akan mencoba menyusun konsep baru yang dapat digunakan dalam mengatasi kompleksitas enkripsi saat ini berdasarkan analisis teknik kriptanalisis Al-Kindi dan relevansinya dengan tantangan enkripsi modern. Konsep-konsep baru ini mungkin melibatkan modifikasi atau pengembangan dari teknik-teknik kriptanalisis Al-Kindi yang ada atau kombinasi dengan teknik-teknik modern yang relevan. Proses penyusunan konsep baru ini akan melibatkan eksplorasi ide-ide inovatif dan pengujian konsep melalui simulasi atau eksperimen yang relevan. Keseluruhan metode penelitian ini bertujuan untuk memperoleh pemahaman yang lebih dalam tentang teknik kriptanalisis Al-Kindi dan relevansinya dengan tantangan enkripsi modern.

## **Hasil dan Pembahasan**

### **Analisis Teknik Kriptanalisis Al-Kindi**

Teknik kriptanalisis Al-Kindi merupakan salah satu pendekatan kuno dalam memecahkan sandi dan menganalisis sistem enkripsi. Al-Kindi, yang dikenal sebagai salah satu ahli matematika dan kriptologi terkemuka pada abad kesepuluh, mengembangkan metode-metode yang inovatif dalam kriptanalisis yang masih relevan hingga saat ini. Salah satu teknik kriptanalisis yang ditemukan oleh Al-Kindi adalah analisis frekuensi. Dalam analisis frekuensi, teks terenkripsi dianalisis berdasarkan frekuensi kemunculan setiap simbol atau huruf dalam teks. Al-Kindi menyadari bahwa dalam bahasa tertentu, terdapat kecenderungan adanya distribusi frekuensi yang konsisten untuk setiap huruf. Dengan membandingkan frekuensi kemunculan huruf dalam teks terenkripsi dengan distribusi frekuensi yang diketahui dalam bahasa tersebut, kita dapat mengidentifikasi pola dan melakukan dekripsi<sup>13</sup>.

Selain analisis frekuensi, Al-Kindi juga menggunakan teknik substitusi dan transposisi dalam kriptanalisis. Teknik substitusi melibatkan penggantian satu simbol atau huruf dengan simbol atau huruf lainnya, sedangkan teknik transposisi

---

<sup>13</sup> Micky Yudi Utama, "Penerapan Matriks Dalam Kriptografi Hill Cipher," *Informatika ITB*, 2016.

melibatkan perubahan urutan huruf dalam teks<sup>14</sup>. Al-Kindi menyadari bahwa kombinasi kedua teknik ini dapat menghasilkan tingkat keamanan yang lebih tinggi. Dalam melakukan kriptanalisis, Al-Kindi mencoba menganalisis pola substitusi dan transposisi yang mungkin digunakan dalam enkripsi dan menggunakan pengetahuan ini untuk memecahkan sandi. Salah satu kekuatan teknik kriptanalisis Al-Kindi adalah kemampuannya dalam mengidentifikasi pola dan menganalisis sistem enkripsi yang menggunakan substitusi dan transposisi. Analisis frekuensi yang dikembangkan oleh Al-Kindi memberikan wawasan yang berharga dalam mengidentifikasi kelemahan dan pola dalam teks terenkripsi. Dengan memahami kecenderungan distribusi frekuensi huruf dalam bahasa tertentu, kita dapat memecahkan sandi dan mendekripsi teks terenkripsi dengan lebih efektif<sup>15</sup>.

Namun, teknik kriptanalisis Al-Kindi juga memiliki beberapa kelemahan. Pertama, teknik ini cenderung kurang efektif dalam menghadapi sistem enkripsi yang lebih kompleks dan canggih, seperti algoritma modern dengan panjang kunci yang besar. Pendekatan Al-Kindi mungkin tidak memadai dalam mengatasi kekuatan enkripsi yang dihasilkan oleh algoritma modern. Selain itu, teknik kriptanalisis Al-Kindi juga dapat memerlukan waktu dan sumber daya yang signifikan untuk menganalisis teks terenkripsi. Karena analisis frekuensi dan metode kriptanalisis Al-Kindi lainnya bergantung pada pengamatan pola dan analisis statistik, diperlukan upaya yang lebih besar untuk menganalisis teks terenkripsi yang lebih panjang dan kompleks<sup>16</sup>.

Dalam menghadapi tantangan enkripsi modern yang semakin kompleks, penting untuk memadukan teknik kriptanalisis Al-Kindi dengan metode dan algoritma kriptografi modern. Integrasi pendekatan kuno dengan pendekatan modern dapat memberikan pendekatan yang holistik dan komprehensif dalam menghadapi sistem enkripsi yang kuat. Kombinasi antara kekuatan teknik kriptanalisis Al-Kindi dalam mengidentifikasi pola dan kelemahan dengan kekuatan algoritma modern dapat membantu dalam memecahkan masalah keamanan yang kompleks dan melindungi data sensitif dengan lebih baik.

### **Hasil Kriptanalisis Al-Kindi Pada Contoh-Contoh Enkripsi Modern yang Diuji**

Dalam penelitian yang dilakukan mengenai kriptanalisis Al-Kindi, hasil kriptanalisis pada contoh-contoh enkripsi modern yang diuji menunjukkan

---

<sup>14</sup> Hernata Rio Cahyo Bawono, "Kriptanalisis Pada Algoritma Cipher Algorithm," *Skripsi* (2015).

<sup>15</sup> Juwita Artanti Kusumaningtyas, "Analisa Algoritma Ciphers Transposition: Study Literature," *Multimatrix* I, no. 1 (2018): 1–12, <http://jurnal.unw.ac.id:1254/index.php/mm/article/view/152/106>.

<sup>16</sup> Ahmad Zaini, "Implementasi Algoritma Super Enkripsi Pada Pengaman Pesan Berbentuk Teks," *Skripsi* (UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM, 2021).

beberapa temuan yang penting. Al-Kindi menggunakan metode analisis frekuensi, substitusi, dan transposisi untuk memecahkan sandi pada contoh-contoh enkripsi modern yang diuji. Salah satu hasil kriptanalisis Al-Kindi adalah kemampuan untuk mengidentifikasi pola dan kelemahan dalam enkripsi modern. Dengan menganalisis frekuensi kemunculan huruf dan pola-pola yang terjadi dalam teks terenkripsi, Al-Kindi dapat mengenali pola-pola yang tidak wajar atau tidak acak<sup>17</sup>. Hal ini memungkinkan untuk menemukan kelemahan dalam metode enkripsi yang digunakan dan mengembangkan strategi untuk memecahkan sandi dengan lebih efisien.

**Gambar 1.** Contoh Code Enkripsi Sederhana

```
def encrypt(message, key):
    encrypted_message = ""
    for char in message:
        if char.isalpha():
            # Men cari posisi huruf dalam alfabet
            position = ord(char.upper()) - ord('A')
            # Menggeser posisi huruf sesuai dengan kunci
            encrypted_position = (position + key) % 26
            # Mendapatkan huruf yang terenkripsi
            encrypted_char = chr(encrypted_position + ord('A'))
            # Menambahkan huruf terenkripsi ke pesan terenkripsi
            encrypted_message += encrypted_char
        else:
            # Menambahkan karakter non-huruf langsung ke pesan terenkripsi
            encrypted_message += char
    return encrypted_message

# Contoh penggunaan
message = "Hello, world!"
key = 3
encrypted_message = encrypt(message, key)
print("Pesan terenkripsi:", encrypted_message)
```

Metode Substitusi

```
def encrypt(message, key):
    encrypted_message = ""
    num_columns = len(key)
    num_rows = (len(message) + num_columns - 1) // num_columns
    # Membangun matriks kosong untuk menyimpan pesan yang terenkripsi
    matrix = [[' ' for _ in range(num_columns)] for _ in range(num_rows)]
    # Mengisi matriks dengan karakter pesan
    for i, char in enumerate(message):
        row = i // num_columns
        col = i % num_columns
        matrix[row][col] = char
    # Membaca matriks secara kolom sesuai dengan urutan kunci
    for col in key:
        for row in range(num_rows):
            encrypted_message += matrix[row][int(col) - 1]
    return encrypted_message

# Contoh penggunaan
message = "Hello, world!"
key = "3124"
encrypted_message = encrypt(message, key)
print("Pesan terenkripsi:", encrypted_message)
```

Metode Transposisi

Hasil kriptanalisis Al-Kindi mengungkapkan pentingnya faktor-faktor non-matematis dalam memecahkan sandi. Al-Kindi menekankan pentingnya pengetahuan tentang bahasa, budaya, dan konteks historis dalam menghadapi tantangan enkripsi modern. Misalnya, pengetahuan tentang kata-kata umum, frasa, atau pola kalimat dalam bahasa tertentu dapat membantu dalam memecahkan sandi yang menggunakan substitusi atau transposisi. Hal ini menunjukkan bahwa dalam menghadapi enkripsi modern, tidak hanya aspek matematis yang perlu diperhatikan, tetapi juga aspek linguistik dan kontekstual. Selain itu, hasil kriptanalisis Al-Kindi juga menunjukkan adanya keterkaitan antara seni kuno kriptanalisis dan tantangan enkripsi modern. Meskipun teknologi dan metode enkripsi telah berkembang pesat sejak zaman Al-Kindi, prinsip-prinsip dasar kriptografi tetap relevan<sup>18</sup>.

<sup>17</sup> Muchlisin Riadi, "Pengertian, Sejarah Dan Jenis Kriptografi," *Kajian Pustaka*, 2014, <https://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html>.

<sup>18</sup> Rifki Sadikin, *Kriptografi Untuk Keamanan Jaringan Dan Implementasinya Dalam Bahasa Java* (Yogyakarta: Penerbit Andi, 2012).

Analisis frekuensi, substitusi, dan transposisi yang dikembangkan oleh Al-Kindi masih dapat digunakan sebagai dasar untuk memahami dan memecahkan enkripsi modern. Hal ini menunjukkan bahwa pendekatan kuno dalam kriptanalisis memiliki nilai penting dalam memahami dan mengatasi tantangan enkripsi modern yang semakin kompleks. Hasil kriptanalisis Al-Kindi pada contoh-contoh enkripsi modern yang diuji menunjukkan bahwa prinsip-prinsip dan metode yang dikembangkan oleh Al-Kindi tetap relevan dalam menghadapi enkripsi modern<sup>19</sup>. Pengetahuan tentang analisis frekuensi, substitusi, transposisi, dan faktor-faktor non-matematis seperti bahasa dan konteks historis dapat memberikan wawasan yang berharga dalam memecahkan sandi dan meningkatkan keamanan enkripsi modern<sup>20</sup>.

### **Kekuatan dan Kelemahan Teknik Kriptanalisis Al-Kindi**

Teknik Kriptanalisis Al-Kindi adalah salah satu metode penting dalam dunia kriptografi yang berfokus pada menganalisis dan memecahkan sandi dalam sistem kriptografi. Metode ini telah digunakan sejak zaman kuno dan terus berkembang seiring berjalannya waktu. Dalam konteks kekuatan, Teknik Kriptanalisis Al-Kindi memiliki beberapa keunggulan yang patut diperhatikan. Salah satu kekuatan utama teknik ini adalah kemampuannya untuk mengidentifikasi pola-pola dalam sandi yang dienkripsi. Dengan menganalisis sekuensi sandi yang panjang, metode ini dapat mengungkap hubungan matematis antara karakteristik sandi dan kunci enkripsi yang digunakan<sup>21</sup>. Dengan demikian, teknik ini mampu memecahkan sandi dengan kecepatan yang relatif tinggi dibandingkan dengan metode kriptanalisis lainnya. Teknik Kriptanalisis Al-Kindi juga memiliki keunggulan dalam mengatasi berbagai jenis enkripsi yang kompleks. Metode ini dapat diterapkan pada berbagai algoritma kriptografi, termasuk yang menggunakan pola penggantian, penggeseran, atau pemangkasan karakter. Kelebihan ini menjadikan teknik ini sangat fleksibel dan dapat digunakan dalam berbagai konteks.

Seperti halnya metode kriptanalisis lainnya, Teknik Kriptanalisis Al-Kindi juga memiliki kelemahan dan batasan yang perlu diperhatikan. Salah satu kelemahan utamanya adalah ketergantungan terhadap jumlah data yang tersedia.

---

<sup>19</sup> Ragil Aria Dewanto and Aries Suharso, "Analisis Teknik-Teknik Kriptografi Terhadap Serangan Jaringan Local," *Jurnal Ilmiah Wahana Pendidikan* 8, no. 16 (2022): 467–76, <https://doi.org/10.5281/zenodo.7068003>.

<sup>20</sup> D Purnamasari, A K Dewi, and A N Trisetiyanto, "Analisis Performansi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data Menggunakan Python Pada Tembang Macapat," *Journal of Systems* 1, no. 2 (2021): 50–54, <https://www.e-journal.ivet.ac.id/index.php/jsite/article/view/2079>.

<sup>21</sup> Febri Dwinata Yonathan, Helfi Nasution, and Heri Priyanto, "Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid Dan Algoritma Kompresi Huffman," *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)* 7, no. 2 (2021): 181, <https://doi.org/10.26418/jp.v7i2.47077>.



Untuk mengungkap pola dan menganalisis sandi dengan akurasi tinggi, diperlukan sejumlah besar data yang cukup signifikan<sup>22</sup>. Jika data yang tersedia terbatas, maka tingkat keberhasilan dalam memecahkan sandi dapat terpengaruh secara signifikan. Teknik Kriptanalisis Al-Kindi juga rentan terhadap serangan brute force atau percobaan-paksa secara sistematis untuk memecahkan sandi. Meskipun teknik ini memiliki kecepatan yang relatif tinggi dalam menganalisis sandi, namun dengan jumlah kombinasi yang besar, proses tersebut dapat memakan waktu yang lama tergantung pada kompleksitas sandi dan sumber daya yang tersedia.

Selanjutnya, seperti halnya banyak teknik kriptanalisis, Teknik Kriptanalisis Al-Kindi juga tidak menjamin keberhasilan dalam semua situasi. Dalam beberapa kasus, enkripsi yang menggunakan algoritma yang sangat rumit dan kuat dapat mempersulit atau bahkan menghambat upaya analisis sandi dengan metode ini. Dalam hal ini, diperlukan pendekatan kriptanalisis yang lebih canggih dan inovatif untuk dapat memecahkan sandi dengan tingkat keberhasilan yang lebih tinggi. Teknik Kriptanalisis Al-Kindi memiliki kekuatan dalam mengidentifikasi pola-pola dalam sandi dan kemampuan untuk mengatasi berbagai jenis enkripsi kompleks. Namun, kelemahan dan batasan seperti ketergantungan pada jumlah data yang tersedia serta rentan terhadap serangan brute force tetap perlu diperhatikan<sup>23</sup>. Dalam mengaplikasikan teknik ini, penting untuk mempertimbangkan konteks dan karakteristik sandi yang sedang dianalisis, serta melibatkan pendekatan kriptanalisis yang lebih canggih guna meningkatkan tingkat keberhasilan dalam memecahkan sandi yang dienkripsi.

Selain kekuatan dan kelemahan yang telah disebutkan sebelumnya, Teknik Kriptanalisis Al-Kindi juga memiliki beberapa aspek tambahan yang perlu dipertimbangkan. Salah satu aspek tersebut adalah ketergantungan terhadap jenis algoritma kriptografi yang digunakan<sup>24</sup>. Meskipun Teknik Kriptanalisis Al-Kindi cukup efektif dalam menguraikan sandi dengan pola penggantian, penggeseran, atau pemangkasan karakter, namun mungkin tidak seefektif dalam mengatasi algoritma enkripsi modern yang lebih kompleks dan kuat. Tingkat keberhasilan Teknik Kriptanalisis Al-Kindi juga sangat dipengaruhi oleh keberadaan atau ketiadaan pengetahuan sebelumnya tentang sistem kriptografi yang digunakan. Jika

---

<sup>22</sup> Fauziah Nur Faqih et al., "Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper Pendahuluan Peningkatan Teknologi Informasi Dan Internet Telah Membuat Banyak Orang Bergantung," *Adijaya Jurnal Multidisiplin* 01, no. 02 (2023): 354–62.

<sup>23</sup> Choirul Huda et al., "Implementasi Algoritma One Time Menggunakan Algoritma Chiper Transposition Sebagai Pengamanan Rahasia Pesan," *Jurnal J-COM (Jurnal ...* 03, no. 01 (2022): 40–48, <https://ejournalunsam.id/index.php/jicom/article/view/4997%0Ahttps://ejournalunsam.id/index.php/jicom/article/download/4997/3171>.

<sup>24</sup> Budi Wijaya Rauf, "Kombinasi Steganografi Bit Matching Dan Kriptografi Playfair Cipher, Hill Cipher Dan Blowfish," *Jurnal Teknologi Informasi* 4, no. 2 (2020): 228–33, <https://doi.org/10.36294/jurti.v4i2.1346>.

analisis memiliki pengetahuan terperinci tentang algoritma enkripsi yang digunakan, termasuk sifat-sifat matematisnya, maka teknik ini dapat lebih efektif dalam memecahkan sandi. Namun, dalam situasi di mana informasi tentang sistem kriptografi tersebut tidak tersedia, tingkat keberhasilan analisis sandi dengan Teknik Kriptanalisis Al-Kindi dapat menurun secara signifikan.

Perlu diperhatikan bahwa Teknik Kriptanalisis Al-Kindi memiliki ketergantungan pada pengujian dan eksperimen yang terus menerus. Analisis sandi yang efektif dengan metode ini sering melibatkan pengujian berulang kali dengan menggunakan sejumlah kombinasi kunci enkripsi yang berbeda. Dalam beberapa kasus, hal ini dapat memakan waktu yang cukup lama dan memerlukan upaya yang intensif untuk memperoleh hasil yang akurat. Dalam prakteknya, Teknik Kriptanalisis Al-Kindi juga dapat membutuhkan sumber daya komputasi yang signifikan. Pemrosesan dan analisis data yang melibatkan sejumlah besar sandi dan kunci enkripsi dapat memerlukan kekuatan komputasi yang tinggi. Oleh karena itu, dalam mengaplikasikan teknik ini, perlu dipertimbangkan ketersediaan sumber daya yang memadai untuk mencapai tingkat keberhasilan yang optimal.

Dalam upaya meningkatkan kekuatan Teknik Kriptanalisis Al-Kindi, penelitian terus dilakukan untuk mengembangkan metode dan pendekatan yang lebih maju dan efektif. Berbagai teknik kriptanalisis modern seperti analisis frekuensi, analisis statistik, atau penggunaan komputer dalam menguraikan sandi menjadi fokus penelitian yang penting. Integrasi Teknik Kriptanalisis Al-Kindi dengan pendekatan-pendekatan ini dapat meningkatkan kemampuan analisis dan memperluas cakupan penerapannya dalam memecahkan sandi yang lebih kompleks. Dengan memahami kekuatan dan kelemahan Teknik Kriptanalisis Al-Kindi secara menyeluruh, kita dapat menyadari betapa pentingnya pemilihan dan penggunaan metode kriptografi yang tepat dalam menjaga keamanan data dan informasi sensitif. Selain itu, pemahaman ini juga dapat menjadi landasan untuk mengembangkan teknik kriptanalisis yang lebih canggih dan efektif di masa depan.

### **Identifikasi Relevansi dengan Tantangan Enkripsi Modern**

Mengintegrasikan prinsip-prinsip Al-Kindi ke dalam sistem-sistem keamanan modern dapat memberikan beberapa peluang yang bernilai. Meskipun teknik kriptanalisis Al-Kindi mungkin tidak secara langsung dapat digunakan untuk memecahkan enkripsi modern yang kuat, prinsip-prinsip yang mendasarinya dapat memberikan wawasan yang berharga dalam perancangan sistem keamanan yang lebih tangguh. Salah satu peluang yang ada adalah menggunakan prinsip analisis frekuensi dalam mendeteksi pola dalam teks terenkripsi. Analisis frekuensi telah terbukti menjadi alat yang efektif dalam memecahkan sandi substitusi kuno. Dalam konteks sistem keamanan modern, prinsip ini dapat digunakan untuk mendeteksi pola anomali dalam teks terenkripsi yang dihasilkan oleh algoritma enkripsi yang

lebih kuat. Dengan mengidentifikasi pola frekuensi yang tidak biasa, dapat dilakukan investigasi lebih lanjut untuk mengungkap potensi kelemahan dalam algoritma enkripsi yang digunakan.

Prinsip substitusi dan transposisi yang digunakan oleh Al-Kindi dapat memberikan inspirasi untuk pengembangan teknik enkripsi modern. Kombinasi dari kedua teknik tersebut dalam bentuk yang lebih kompleks dan kuat dapat memberikan keamanan yang lebih baik terhadap serangan kriptanalisis. Penggabungan prinsip-prinsip Al-Kindi dengan metode kriptografi modern dapat menghasilkan algoritma yang lebih tangguh dan tahan terhadap serangan. Peluang lainnya adalah dalam pengembangan metode kriptanalisis yang lebih canggih. Studi tentang teknik kriptanalisis Al-Kindi dapat memberikan wawasan tentang prinsip-prinsip dasar yang tetap relevan dalam memahami enkripsi modern. Dengan mempelajari pendekatan kuno seperti Al-Kindi, kita dapat mengidentifikasi celah dan kelemahan dalam metode enkripsi modern yang sering kali didasarkan pada prinsip-prinsip matematika yang kompleks. Ini dapat mengarah pada pengembangan metode kriptanalisis yang lebih canggih untuk mengatasi enkripsi modern yang semakin kuat<sup>25</sup>.

Mengintegrasikan prinsip-prinsip Al-Kindi ke dalam sistem-sistem keamanan modern dapat memberikan peluang untuk meningkatkan keamanan dan ketahanan terhadap serangan kriptanalisis. Meskipun prinsip-prinsip ini tidak dapat digunakan secara langsung dalam memecahkan enkripsi modern yang kuat, mereka dapat memberikan panduan dalam mendeteksi kelemahan, mengembangkan teknik enkripsi yang lebih kuat, dan memperkaya pemahaman kita tentang kriptanalisis secara keseluruhan. Dengan pendekatan yang holistik yang menggabungkan prinsip-prinsip kuno dan teknik-teknik modern, kita dapat mencapai keamanan yang lebih baik dalam menghadapi tantangan enkripsi yang semakin kompleks.

Teknik kriptanalisis Al-Kindi memiliki relevansi yang signifikan dengan tantangan enkripsi modern yang dihadapi dalam era digital saat ini. Meskipun Al-Kindi hidup pada zaman kuno, prinsip-prinsip dan metode yang dikembangkannya tetap memiliki relevansi dalam mengatasi masalah keamanan yang kompleks yang dihadapi dalam enkripsi modern. Salah satu relevansi utama teknik kriptanalisis Al-Kindi dengan tantangan enkripsi modern adalah dalam pemahaman terhadap prinsip-prinsip dasar kriptografi. Al-Kindi mengembangkan metode seperti analisis frekuensi, substitusi, dan transposisi, yang merupakan dasar-dasar dalam enkripsi modern. Pemahaman yang kuat tentang prinsip-prinsip ini memungkinkan para ahli kriptografi untuk mengenali kelemahan dalam sistem enkripsi modern,

---

<sup>25</sup> Selli Oktavani, Fahrizal Rizky, and Indra Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar ( AES ) JURNAL MEDIA INFORMATIKA [ JUMIN ]" 4 (2023): 97–101.

mengembangkan metode dekripsi yang lebih efektif, dan menguji tingkat keamanan suatu algoritma enkripsi<sup>26</sup>.

Teknik kriptanalisis Al-Kindi juga relevan dalam menghadapi tantangan enkripsi modern karena memungkinkan identifikasi pola dan kelemahan dalam teks terenkripsi. Meskipun algoritma enkripsi modern cenderung lebih kompleks dan menggunakan metode yang lebih maju, analisis frekuensi dan teknik lain yang dikembangkan oleh Al-Kindi dapat membantu dalam mengidentifikasi pola yang tidak biasa atau kelemahan yang mungkin ada dalam teks terenkripsi. Dengan memahami prinsip-prinsip kriptanalisis kuno, para ahli keamanan dapat mengembangkan metode analisis yang lebih canggih untuk menghadapi tantangan enkripsi modern yang semakin kompleks. Pendekatan kuno terhadap kriptanalisis juga memiliki relevansi dalam menghadapi tantangan enkripsi modern karena memberikan perspektif yang berbeda dan inovatif<sup>27</sup>. Metode kriptanalisis yang dikembangkan oleh Al-Kindi berdasarkan pemikiran kreatif dan solusi yang tidak konvensional. Pemahaman tentang metode ini memungkinkan para ahli kriptografi untuk berpikir di luar kotak dalam mencari solusi untuk masalah keamanan yang kompleks dan mengatasi teknik-teknik enkripsi modern yang semakin canggih.

Relevansi teknik kriptanalisis Al-Kindi dengan tantangan enkripsi modern juga terletak pada pengembangan teknik-teknik kriptanalisis modern yang lebih kuat. Dengan mempelajari prinsip-prinsip kriptanalisis kuno, para ahli keamanan dapat mengidentifikasi kelemahan dalam enkripsi modern dan memperkuat lapisan keamanan dengan memperbaiki dan mengembangkan teknik-teknik yang ada. Integrasi prinsip-prinsip kriptanalisis kuno ke dalam teknik-teknik modern juga dapat memberikan pendekatan yang lebih holistik dalam mengembangkan algoritma enkripsi yang lebih tangguh dan tahan terhadap serangan. Teknik kriptanalisis Al-Kindi memiliki relevansi yang signifikan dengan tantangan enkripsi modern. Pemahaman prinsip-prinsip dasar, kemampuan identifikasi pola dan kelemahan, pendekatan kreatif, dan pengembangan teknik-teknik kriptanalisis modern yang lebih kuat merupakan beberapa aspek relevan yang diperoleh dari pendekatan kriptanalisis kuno. Dengan menggabungkan kebijaksanaan masa lalu dengan teknologi modern, kita dapat menghadapi tantangan enkripsi modern dengan lebih baik dan meningkatkan keamanan sistem keamanan informasi di dunia yang terus berkembang ini.

---

<sup>26</sup> Adisya Poeja Kehista et al., “Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce : Ancaman , Risiko , Strategi Kemanan ( Literature Review )” 4, no. 5 (2023): 625–32.

<sup>27</sup> Desi Fitriani Ningrum et al., “Implementasi Keamanan Data Menggunakan Kriptografi Caesar Chiper Desi,” *Adijaya Jurnal Multidisiplin* 01, no. 02 (2016): 1–23.

### **Penyusunan Konsep Baru**

Dalam menghadapi tantangan enkripsi modern yang semakin kompleks, diperlukan pendekatan yang inovatif dan kreatif dalam mengembangkan konsep baru dalam kriptanalisis. Melalui pemahaman tentang prinsip-prinsip kriptografi yang ada dan penerapan teknologi terbaru, kita dapat menyusun konsep baru yang dapat meningkatkan keamanan dan efektivitas dalam memecahkan sandi. Konsep baru yang dapat dikembangkan adalah penggunaan kecerdasan buatan (AI) dalam kriptanalisis. Dengan kemajuan dalam bidang AI dan machine learning, kita dapat melatih model-model komputer untuk secara otomatis menganalisis teks terenkripsi, mengidentifikasi pola, dan mencari solusi yang efisien untuk memecahkan sandi. Dengan memanfaatkan kecerdasan buatan, kita dapat mengatasi keterbatasan dalam analisis manusia yang mungkin memakan waktu dan sumber daya yang besar. Konsep ini dapat memberikan keuntungan dalam memecahkan sandi dengan cepat dan efektif, terutama dalam menghadapi teks terenkripsi yang lebih panjang dan rumit.

Konsep baru juga dapat melibatkan penggunaan teknologi blockchain dalam kriptanalisis. Dalam sistem blockchain, data terenkripsi diubah menjadi blok-blok yang terhubung dan dijamin keamanannya melalui mekanisme konsensus. Dengan memanfaatkan keandalan dan keamanan blockchain, kita dapat mengembangkan metode kriptanalisis yang dapat digunakan untuk memverifikasi keaslian data dan memastikan integritas informasi dalam konteks blockchain. Konsep ini dapat membantu dalam mengatasi tantangan enkripsi modern yang terkait dengan keamanan dan keaslian data. Selain itu, pendekatan interdisipliner juga dapat menyusun konsep baru dalam kriptanalisis. Dengan menggabungkan pengetahuan dari berbagai bidang seperti matematika, komputer, statistik, dan psikologi, kita dapat mengembangkan pendekatan yang holistik dalam memecahkan sandi. Misalnya, penggunaan teknik-teknik analisis data dan pembelajaran mesin dari ilmu komputer, atau penggunaan prinsip-prinsip psikologi untuk memahami pola perilaku pengguna dalam penggunaan kata sandi. Pendekatan interdisipliner seperti ini dapat memberikan wawasan baru dan solusi yang lebih efektif dalam menghadapi tantangan enkripsi modern.

Konsep baru juga dapat melibatkan pengembangan algoritma kriptografi yang lebih kuat dan inovatif. Dalam menghadapi tantangan enkripsi modern yang semakin kompleks, diperlukan pengembangan algoritma yang dapat menghasilkan keamanan yang lebih tinggi dan tahan terhadap serangan. Konsep baru dapat melibatkan pengembangan algoritma kriptografi berbasis quantum, yang dapat menghadapi serangan dari komputer kuantum yang kuat di masa depan. Selain itu, pengembangan algoritma yang menggabungkan teknik-teknik kriptanalisis kuno dengan metode modern seperti kecerdasan buatan dan blockchain juga dapat menjadi konsep baru yang menarik. Dalam menyusun konsep baru dalam

kriptanalisis, penting untuk menjaga keseimbangan antara keamanan, efisiensi, dan keterjangkauan. Konsep baru harus memberikan tingkat keamanan yang tinggi dalam melindungi data sensitif, tetapi juga harus efisien dalam memecahkan sandi dengan waktu yang wajar. Selain itu, konsep baru harus dapat diimplementasikan secara praktis dan terjangkau dalam skala yang luas.

### **Simpulan**

Dalam penelitian ini, telah dilakukan kajian ulang terhadap teknik kriptanalisis Al-Kindi dengan tujuan menghubungkan seni kuno kriptanalisis dengan tantangan enkripsi modern. Melalui hasil penelitian ini, berbagai temuan yang signifikan telah ditemukan, serta kontribusi yang berharga terhadap pemahaman tentang kriptanalisis telah diberikan. Temuan penelitian ini mengungkapkan bahwa teknik kriptanalisis Al-Kindi masih relevan dalam menghadapi enkripsi modern. Meskipun metode-metode enkripsi modern menggunakan algoritma kompleks dan kunci yang panjang, prinsip-prinsip Al-Kindi seperti analisis frekuensi, substitusi, dan transposisi tetap memberikan wawasan berharga dalam mengidentifikasi pola dan menguji kekuatan enkripsi. Dalam konteks pengujian penetrasi dan analisis kelemahan sistem keamanan modern, integrasi prinsip-prinsip Al-Kindi dapat membantu dalam mengidentifikasi kerentanan dan meningkatkan keamanan. Kontribusi utama dari penelitian ini adalah dalam menghubungkan seni kuno kriptanalisis dengan tantangan enkripsi modern. Prinsip-prinsip Al-Kindi yang terinspirasi dari seni dan matematika kuno membuka jalan untuk berpikir secara kreatif dan inovatif dalam mengembangkan solusi untuk masalah keamanan modern.

Selain itu, penelitian ini juga menunjukkan pentingnya mempertimbangkan prinsip-prinsip kriptanalisis kuno sebagai landasan untuk pengembangan teknik-teknik kriptanalisis modern yang lebih kuat. Integrasi prinsip-prinsip Al-Kindi ke dalam sistem-sistem keamanan modern menawarkan peluang untuk meningkatkan kekuatan enkripsi, mengidentifikasi kelemahan, mengembangkan algoritma yang lebih aman, dan memperluas pendekatan dalam memecahkan masalah keamanan yang kompleks. Meskipun teknologi enkripsi modern telah mengalami kemajuan pesat, prinsip-prinsip dasar kriptanalisis yang telah ada sejak zaman kuno tetap relevan dan berharga dalam konteks keamanan digital saat ini. Dengan mempelajari pendekatan kuno, kita dapat memahami dasar-dasar teknik-teknik enkripsi dan bagaimana algoritma-algoritma modern memanfaatkannya. Hal tersebut memungkinkan untuk lebih memahami kelemahan dan potensi kerentanan yang mungkin ada dalam sistem enkripsi modern. Dalam menghadapi kompleksitas keamanan digital, pendekatan kuno memberikan wawasan, inspirasi, dan fondasi yang kuat untuk pengembangan teknik-teknik kriptanalisis modern. Dengan memadukan pengetahuan masa lalu dengan teknologi dan pendekatan yang ada,

dapat melangkah maju dalam menciptakan sistem keamanan yang lebih tangguh dan melindungi informasi sensitif di dunia yang semakin terhubung dan rentan.

### **Daftar Sumber**

- Al-kazaz, Noor R. *Compression-Based Methods for the Automatic Cryptanalysis of Classical Ciphers College of Environmental Sciences and Engineering Compression-Based Methods for the Automatic Cryptanalysis of Classical* Noor R. Al-Kazaz. Bangor University, 2020.
- Albert Ginting, R. Rizal Isnanto, and Ike Pertiwi Windasari. "Implementasi Algoritma Kriptografi RSA Untuk Enkripsi Dan Dekripsi Email." *Jurnal Teknologi Dan Sistem Komputer* 3, no. 2 (2015): 253–58. <https://jtsiskom.undip.ac.id/article/view/12009>.
- Bawono, Hernata Rio Cahyo. "Kriptanalisis Pada Algoritma Cipher Algorithm." *Skripsi*, 2015.
- Dewanto, Ragil Aria, and Aries Suharso. "Analisis Teknik-Teknik Kriptografi Terhadap Serangan Jaringan Local." *Jurnal Ilmiah Wahana Pendidikan* 8, no. 16 (2022): 467–76. <https://doi.org/10.5281/zenodo.7068003>.
- Fajrin, Ricky Maulana, Jalan Kolonel, Wahid Udin, Kayuara Sekayu, and Musi Banyuasin. "Keamanan Data Pada Cloud Computing." *Seminar Nasional Teknologi Informasi, Komunikasi Dan Manajemen Palembang-Indonesia* 23 (2014).
- Faqih, Fauziah Nur, Muhlis Tahir, Zarwanda Ashfarina, and Robby Irsyad. "Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper Pendahuluan Peningkatan Teknologi Informasi Dan Internet Telah Membuat Banyak Orang Bergantung." *Adijaya Jurnal Multidisiplin* 01, no. 02 (2023): 354–62.
- Huda, Choirul, Dadang Iskandar Mulyana, Aji Dwi Prasetyo, and Ali Yafi Zulkarnain. "Implementasi Algoritma One Time Menggunakan Algoritma Chipper Transposition Sebagai Pengamanan Rahasia Pesan." *Jurnal J-COM (Jurnal ...* 03, no. 01 (2022): 40–48. <https://ejurnalunsam.id/index.php/jicom/article/view/4997%0Ahttps://ejurnalunsam.id/index.php/jicom/article/download/4997/3171>.
- Kaniawulan, Ismi, M Rafi Muttaqin, and Dhiya Ulhaq. "Sistem Manajemen Pengetahuan Forum Diskusi Dosen Knowledge Management System of Lecturer Discussion Forum." *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIK)* 7, no. 1 (2020): 51–58. <https://doi.org/10.25126/jtiik.202071258>.
- Kehista, Adisya Poeja, Achmad Fauzi, Annisa Tamara, Ivanida Putri, and Nurul Afni. "Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce : Ancaman , Risiko , Strategi Kemanan ( Literature Review )" 4, no. 5 (2023): 625–32.
- Kusumaningtyas, Juwita Artanti. "Analisa Algoritma Ciphers Transposition : Study Literature." *Multimatrix* I, no. 1 (2018): 1–12. <http://jurnal.unw.ac.id:1254/index.php/mm/article/view/152/106>.
- Laskari, Elena C., G. C. Meletiou, Y. C. Stamatou, and M. N. Vrahatis. *Cryptography and Cryptanalysis through Computational Intelligence. Studies in Computational Intelligence*. Vol. 57, 2007. [---

169 | \*Historia Madania\* Volume 7 \(2\) 2023](https://doi.org/10.1007/978-3-</a></p></div><div data-bbox=)

540-71078-3\_1.

- Mahto, Dindayal, and Dilip Kumar Yadav. "RSA and ECC, A Comparative Analysis. Pdf." *International Journal of Applied Engineering Research* 12, no. 19 (2017): 9053–61.
- Ningrum, Desi Fitriani, Muhlis Tahir, Wahyu Dwi Angelina, Eliza Permatasari, Fifi Rinazah Rofiq, Miftakhul Hidayati, Fatimatus Sahroh, Andi Setiawan, and Desifitriani733@gmail.com. "Implementasi Keamanan Data Menggunakan Kriptografi Caesar Cipher." *Adijaya Jurnal Multidisiplin* 01, no. 02 (2016): 1–23.
- Oktavani, Selli, Fahrizal Rizky, and Indra Gunawan. "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar ( AES ) JURNAL MEDIA INFORMATIKA [ JUMIN ]" 4 (2023): 97–101.
- Purnamasari, D, A K Dewi, and A N Trisetiyanto. "Analisis Performansi Kriptografi Berbasis Caesar Cipher Untuk Keamanan Data Menggunakan Python Pada Tembang Macapat." *Journal of Systems* 1, no. 2 (2021): 50–54. <https://www.e-journal.ivet.ac.id/index.php/jsite/article/view/2079>.
- Raodia, Raodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019): 39. <https://doi.org/10.24252/jurisprudentie.v6i2.11399>.
- Rauf, Budi Wijaya. "Kombinasi Steganografi Bit Matching Dan Kriptografi Playfair Cipher, Hill Cipher Dan Blowfish." *Jurnal Teknologi Informasi* 4, no. 2 (2020): 228–33. <https://doi.org/10.36294/jurti.v4i2.1346>.
- Renaldy, Aldi, Achmad Fauzi, An Nisaa Shabrina, and Hanny Novita Ramadhan. "Peran Sistem Informasi Dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan." *Jurnal Ilmu Multidisiplin* 2, no. 1 (2023): 15–22.
- Riadi, Muchlisin. "Pengertian, Sejarah Dan Jenis Kriptografi." *Kajian Pustaka*, 2014. <https://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html>.
- Sadikin, Rifki. *Kriptografi Untuk Keamanan Jaringan Dan Implementasinya Dalam Bahasa Java*. Yogyakarta: Penerbit Andi, 2012.
- Sulistyo, Budi. *Kriptanalisis Cipher Blok Berdasarkan Permainan Kaotik*. Vol. 33204013. Bandung: INSTITUT TEKNOLOGI BANDUNG, 2009.
- Suyanto, S. "Keamanan Database Menggunakan Metode Enkripsi." *Jurnal Ilmiah Matrik*, no. 12 (2012): 137–50.
- Utama, Micky Yudi. "Penerapan Matriks Dalam Kriptografi Hill Cipher." *Informatika ITB*, 2016.
- Wiharto, Yudi, and Ari Irawan. "Enkripsi Data Menggunakan AES 256." *Jurnal Kilat* 7, no. 2 (2018): 91–99.
- Yonathan, Febri Dwinata, Helfi Nasution, and Heri Priyanto. "Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid Dan Algoritma Kompresi Huffman." *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)* 7, no. 2 (2021): 181. <https://doi.org/10.26418/jp.v7i2.47077>.
- Zaini, Ahmad. "Implementasi Algoritma Super Enkripsi Pada Pengaman Pesan



*Integrasi Seni Kuno dan Tantangan Enkripsi Modern melalui Kajian Ulang Teknik Kriptanalisis Al-Kindi | Anatansyah Ayomi Anandari, Rudy Agus Gemilang Gultom*

Berbentuk Teks.” *Skripsi*. UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM, 2021.