JIKUM
JURNAL ILMU KOMPUTER

**E-ISSN: 9999-9999**
**Volume** 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

# Implementasi Sistem Keamanan Data Menggunakan Algoritma Kriptografi Asimetris *Elliptic Curve Cryptography* (ECC) Berbasis Website

**Putri Iqlima[1], Muhammad Rayyan[2], Az Zahra Alfansuri Rambe[3], Elin Ardina[4], Delia Fitri Anggriani Lubis[5], Dea Ismawati[6]**
[1,2,3,4,5,6]Universitas Malikussaleh, Indonesia
[1]putriiqlima04@email.com, [2]muhammadrayyan040399@email.com, [3]azzahraalfansuri01@email.com, [4]elinardina4@email.com, [5]deliafitrianggrianilubis@gmail.com , [6]ismawatidea110@gmail.com

**ABSTRACT**

*Data security is very important in the digital world, especially to protect personal data, financial transactions, and sensitive communications. One method used to maintain information security is cryptography, specifically Elliptic Curve Cryptography (ECC). ECC offers a level of security equivalent to other algorithms such as RSA, but with a smaller key size, making it more efficient in resource usage. This web-based system allows users to encrypt and decrypt messages using public and private keys. Although effective in maintaining data security, this system still requires manual input of keys by the user, which is prone to errors. Further development is needed to improve key management and user convenience.*

**Kata Kunci:**
*Data security, Cryptography, Elliptic Curve Cryptography (ECC)*

## PENDAHULUAN

Keamanan data adalah aspek yang sangat penting dalam dunia digital saat ini, terutama dengan semakin meningkatnya jumlah transaksi dan pertukaran informasi melalui internet. Untuk melindungi data pribadi, transaksi keuangan, dan komunikasi sensitif dari ancaman yang terus berkembang, diperlukan pengamanan informasi yang efisien dan terpercaya, salah satunya melalui sistem enkripsi. Kriptografi merupakan salah satu disiplin ilmu yang berperan dalam menjaga keamanan informasi. Dengan menggunakan kriptografi, informasi yang dianggap rahasia dapat disembunyikan menggunakan teknik penyandian, sehingga hanya dapat dipahami oleh pengirim dan penerima yang berwenang, sementara pihak lain tidak dapat mengerti isi informasi tersebut (Nugroho & Painem, 2022). Kriptografi dapat dibagi menjadi dua kategori utama, yaitu kriptografi kunci simetris dan kriptografi kunci asimetris. Dalam kriptografi kunci simetris, kunci yang sama digunakan untuk mengenkripsi pesan (*plaintext*) dan mendekripsi pesan yang sudah terenkripsi (*ciphertext*). Sementara itu, kriptografi kunci asimetris melibatkan dua kunci yang berbeda, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk mengenkripsi pesan, sehingga siapa saja yang ingin mengirim pesan secara rahasia dapat menggunakan kunci tersebut. Di sisi lain, kunci pribadi disimpan dengan aman dan hanya diketahui oleh pemiliknya, sehingga hanya mereka yang dapat mendekripsi *ciphertext* yang telah dihasilkan dengan kunci publik (Perdana et al., 2022). Berbagai metode kriptografi telah digunakan untuk memastikan keamanan data, dan salah satu yang paling menjanjikan adalah *Elliptic Curve Cryptography* (ECC).

*Elliptic Curve Cryptography* (ECC) adalah salah satu pendekatan algoritma kriptografi kunci publik berdasarkan pada struktur aljabar dari kurva elips pada daerah finite (Nugroho & Painem, 2022). Sistem kriptografi berbasis kurva elips menawarkan perlindungan yang lebih kuat dan lebih efektif dibandingkan algoritma enkripsi lainnya dalam mencegah serangan. Dengan demikian, sistem ini membuat situs web dan infrastruktur lebih aman dibandingkan metode enkripsi tradisional. ECC memberikan jaminan yang lebih baik untuk keamanan di dunia internet seluler. Selain itu, kriptografi kurva elips juga lebih sesuai untuk aplikasi di internet seluler karena memiliki panjang kunci yang relatif pendek, yaitu hanya 256 bit (Indriyani et al., 2023).

Implementasi ECC dalam sistem berbasis website dapat dilakukan melalui berbagai cara, seperti autentikasi pengguna, enkripsi pesan, dan pengelolaan sertifikat digital. Penggunaan kunci publik dan kunci pribadi dalam ECC memungkinkan pengamanan data yang lebih efektif. Seiring dengan meningkatnya ketergantungan kita pada teknologi digital, penerapan ECC menjadi semakin relevan, terutama dalam konteks *Internet of Things* (IoT) dan aplikasi berbasis web yang memerlukan tingkat keamanan tinggi untuk melindungi data penggunanya. Oleh karena itu, penelitian lebih lanjut dan penerapan praktis mengenai penggunaan ECC dalam sistem-sistem ini sangatlah penting untuk membangun infrastruktur yang lebih aman di era digital yang terus berkembang.

## TINJAUAN PUSTAKA

### Keamanan Data

Keamanan adalah keadaan di mana kita terbebas dari bahaya. Istilah ini sering digunakan dalam konteks kejahatan dan berbagai bentuk kecelakaan. Dalam hal ini, keamanan data merupakan hal yang sangat penting untuk

JIKUM
JURNAL ILMU KOMPUTER
**E-ISSN: 9999-9999**
**Volume** 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

menjaga kerahasiaan informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja. Terlebih lagi, ketika pengiriman informasi dilakukan melalui jaringan publik, jika data tersebut tidak dilindungi dengan baik, sangat mungkin bagi pihak-pihak yang tidak bertanggung jawab untuk menyadap dan mengakses isi informasi tersebut (Husaini et al., 2022).

**Kriptografi**

*Criptography* berasal dari bahasa Yunani, yang terdiri dari dua kata, yaitu "*kripto*" yang berarti rahasia dan "*graphia*" yang berarti tulisan. Dalam terminologinya, kriptografi dapat dipahami sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari satu lokasi ke lokasi lain, isi pesan tersebut berpotensi disadap oleh pihak yang tidak berwenang. Untuk melindungi keamanan pesan, informasi tersebut dapat diacak atau diubah menjadi kode yang sulit dipahami oleh orang lain. Tujuan utama dari sistem kriptografi mencakup keaslian (*Authentication*), integritas (*Integrity*), otoritas (*Authority*), dan tidak dapat disangkal (*Non-repudiation*). Proses enkripsi dan dekripsi didasarkan pada hubungan matematis antara dua himpunan, yaitu himpunan yang berisi elemen *plainteks* dan himpunan yang berisi elemen *ciphertext* (Azlin et al., 2018).

**Kriptografi Asimetris**

Kriptografi asimetris merupakan salah satu jenis kriptografi yang menggunakan dua kunci berbeda namun saling berhubungan, yaitu kunci publik dan kunci privat. Kunci publik berfungsi untuk mengenkripsi pesan, sementara kunci privat dipakai untuk mendekripsi pesan tersebut. Dua contoh algoritma kriptografi asimetris yang banyak digunakan adalah RSA (*Rivest-Shamir-Adleman*) dan ECC (*Elliptic Curve Cryptography*). Kelebihan utama dari kriptografi asimetris adalah kemampuannya untuk mendukung komunikasi yang aman tanpa perlu membagikan kunci secara langsung (Alfatah et al., n.d.).

***Elliptic Curve Cryptography* (ECC)**

*Elliptic Curve Cryptography* (ECC) adalah salah satu algoritma yang digunakan untuk mengamankan data di komputer. Algoritma ini dikembangkan oleh Victor Miller dan Neal Koblitz pada tahun 1985. Keunggulan utama ECC dibandingkan dengan algoritma kriptografi RSA terletak pada penggunaan kunci yang lebih pendek, sementara tingkat keamanannya tetap setara (Taopan et al., 2022).

**Implementasi Kriptografi pada Aplikasi Web**

Penggunaan kriptografi pada aplikasi web bertujuan untuk memastikan bahwa data yang dikirimkan antar pengguna dan server tetap aman. Implementasi kriptografi berbasis web meliputi enkripsi data, autentikasi pengguna, dan pengelolaan sertifikat digital. Dengan menggunakan algoritma ECC, sistem berbasis web dapat meningkatkan keamanan komunikasi data, sambil tetap mempertahankan performa tinggi berkat ukuran kunci yang lebih kecil dan proses komputasi yang lebih ringan.

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan rekayasa perangkat lunak dengan metode eksperimen. Implementasi dilakukan dengan membangun sistem enkripsi dan dekripsi pesan berbasis website menggunakan algoritma *Elliptic Curve Cryptography* (ECC).

**Desain Sistem**

Sistem dikembangkan dalam bentuk aplikasi web yang memungkinkan pengguna melakukan:

a. Input pesan
b. Enkripsi menggunakan kunci publik ECC
c. Dekripsi menggunakan kunci privat ECC
d. Proses kriptografi utama dilakukan dengan Python, sedangkan antarmuka pengguna dan integrasi web menggunakan PHP.

**Tahapan Penelitian**

Tahapan dalam penelitian ini meliputi:

a. Menentukan kebutuhan fungsional sistem.
b. Membuat desain antarmuka dan alur proses enkripsi-dekripsi.
c. Menjalankan script Python untuk menghasilkan pasangan kunci ECC.
d. Kunci publik dan privat ditampilkan melalui terminal.
e. Pengguna menyalin kunci yang dihasilkan dari Python ke dalam form web.
f. Melakukan pengujian fungsi enkripsi dan dekripsi untuk memastikan keamanan dan keakuratan data.

JIKUM
JURNAL ILMU KOMPUTER
**E-ISSN: 9999-9999**
**Volume** 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

**Alat dan Bahan**

a. Bahasa Pemrograman: Python 3.10, PHP 8, HTML5 dan CSS3.
b. Library python: cryptography.hazmat.primitives.asymmetric.ec, cryptography.hazmat.primitives.serialization, cryptography.hazmat.primitives.hashes, cryptography.hazmat.primitives.asymmetric.padding, dan base64.
c. Server: XAMPP (Apache dan MySQL)

**Teknik Pengujian**

Pengujian dilakukan dengan metode *black box testing*, yaitu memverifikasi apakah:

a. Pesan berhasil dienkripsi menggunakan kunci publik.
b. Pesan dapat didekripsi dengan benar menggunakan kunci privat.
c. Sistem gagal mendekripsi jika menggunakan kunci yang tidak valid.

## HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan sistem keamanan data berbasis website yang menggunakan algoritma *Elliptic Curve Cryptography* (ECC) untuk enkripsi dan dekripsi pesan. Pembuatan pasangan kunci publik dan privat dilakukan menggunakan bahasa pemrograman Python dengan library cryptography.hazmat, sedangkan proses pengolahan pesan dilakukan melalui aplikasi berbasis PHP.

Pembuatan kunci ECC diawali dengan pembuatan kunci privat menggunakan metode *generate_private_key* dari modul ec, dengan kurva SECP256R1. Setelah itu, kunci publik diperoleh dari kunci privat yang telah dibuat. Kunci-kunci ini kemudian diserialisasi ke dalam format PEM agar dapat dengan mudah dibaca dan disimpan dalam bentuk teks. Berikut adalah potongan kode Python untuk proses pembuatan kunci:

app.py

```python
from cryptography.hazmat.primitives.asymmetric import ec
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
import base64

private_key = ec.generate_private_key(ec.SECP256R1())
public_key = private_key.public_key()

private_pem = private_key.private_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PrivateFormat.PKCS8,
    encryption_algorithm=serialization.NoEncryption()
)

public_pem = public_key.public_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PublicFormat.SubjectPublicKeyInfo
)
```

Gambar 1. Kode Python Pembuatan Kunci

Jadi, untuk hasil kuncinya sebagai berikut:

TERMINAL

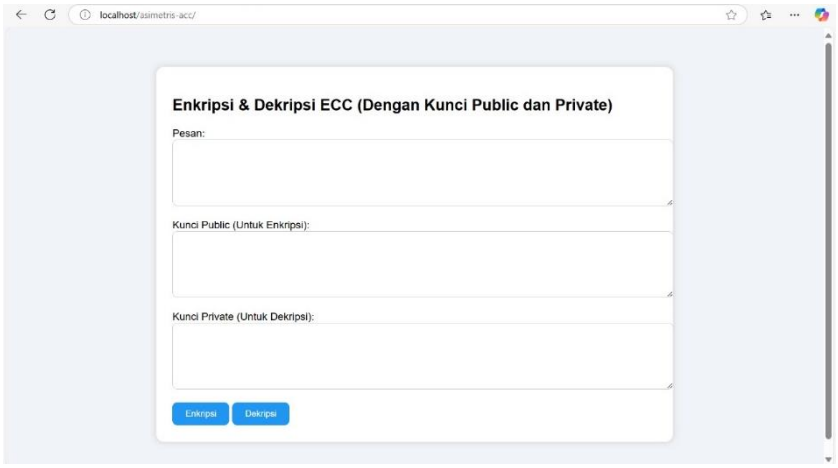
```
PS D:\xampp\htdocs\asimetris-acc> python app.py
Private Key:
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQguWLd8vAFGLgz64nA
P1xiKtBSAwkX4w/0fYoigM2w0IShRANCAARfK5uyrwaW8nzkK1aTm6kG0Fz2w3H1
/9qyYTNHej83wOu5xCAPnwd7KDhjhRtAuOQPKkxfGd2VkARzxJI/E60R
-----END PRIVATE KEY-----


Public Key:
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEXyubsq8GlvJ85CtWk5upBtBc9sNx
9f/asmEzR3o/N8DrucQgD58Heyg4Y4UbQLjkDypMXxndlZAEc8SSPxOtEQ==
-----END PUBLIC KEY-----
```

Gambar 2. Hasil Kunci

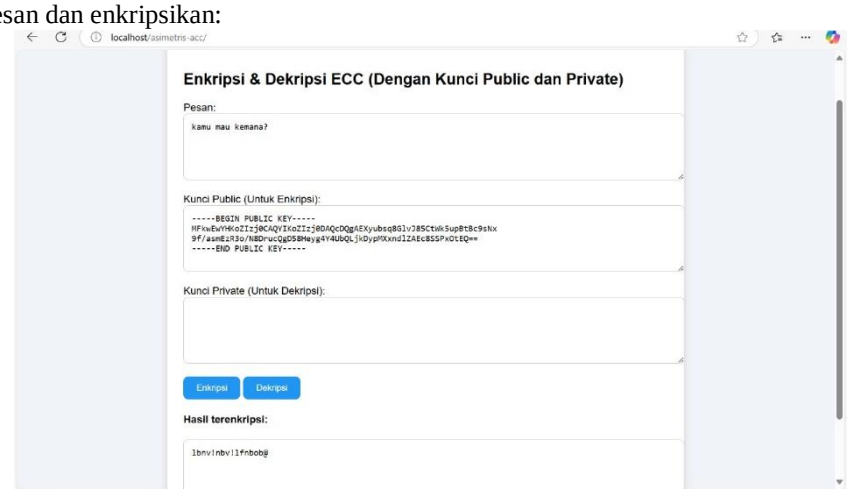
Di sisi aplikasi web, pengguna cukup memasukkan pesan dan kunci publik untuk melakukan enkripsi, dan menggunakan kunci privat untuk dekripsi. Antarmuka web yang sederhana memungkinkan pengguna mengoperasikan enkripsi dan dekripsi pesan dengan cepat.

JIKUM
JURNAL ILMU KOMPUTER
**E-ISSN: 9999-9999**
**Volume** 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx




Gambar 3. Antarmuka Website

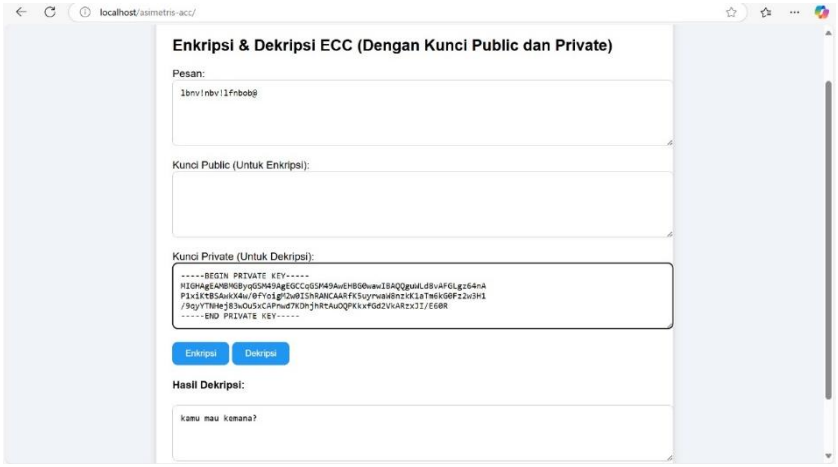
Masukkan pesan dan enkripsikan:




Gambar 4. Pesan Enkripsi

Contoh hasil enkripsi dari pesan "kamu mau kemana?" menghasilkan *ciphertext* berupa karakter-karakter acak yang tidak dapat dibaca secara langsung.

Sebaliknya, dekripsi dengan kunci yang benar berhasil mengembalikan pesan ke bentuk aslinya.




Gambar 5. Pesan Dekripsi

JIKUM
JURNAL ILMU KOMPUTER

**E-ISSN: 9999-9999**
**Volume** 1, **Number** 1, Mei 2025
https://doi.org/10.62671/jikum.vxix.xxxx

Penggunaan ECC dalam sistem ini terbukti sangat efektif, karena hanya memerlukan panjang kunci 256 bit untuk mencapai tingkat keamanan setara dengan RSA 3072 bit. Hal ini secara signifikan mengurangi kebutuhan memori dan meningkatkan kecepatan proses, menjadikannya sangat ideal untuk aplikasi berbasis web serta perangkat dengan sumber daya terbatas.

Namun, sistem ini masih memerlukan input kunci secara manual dari pengguna, yang membuatnya rentan terhadap kesalahan manusia. Oleh karena itu, pengembangan lebih lanjut seperti manajemen kunci otomatis atau integrasi sertifikat digital dapat menjadi solusi untuk mengatasi keterbatasan tersebut.

Secara keseluruhan, penerapan ECC berbasis website ini telah berhasil menunjukkan efektivitasnya dalam menjaga integritas, keaslian, dan kerahasiaan data dalam lingkungan web.

## KESIMPULAN

Penerapan *Elliptic Curve Cryptography* (ECC) dalam sistem enkripsi dan dekripsi pesan berbasis web berhasil menunjukkan efektivitasnya dalam menjaga keamanan data. ECC menawarkan keamanan yang setara dengan algoritma kriptografi lain seperti RSA, namun dengan ukuran kunci yang lebih kecil, sehingga lebih efisien dalam penggunaan sumber daya, baik dari segi memori maupun kecepatan. Sistem ini memungkinkan enkripsi dan dekripsi pesan yang aman menggunakan kunci publik dan privat, yang hanya dapat diproses dengan kunci yang sesuai.

Meskipun hasilnya memuaskan, sistem ini masih memerlukan input manual dari pengguna untuk memasukkan kunci, yang berpotensi menambah risiko kesalahan. Oleh karena itu, perlu adanya pengembangan lebih lanjut, seperti penerapan manajemen kunci otomatis atau sertifikat digital, untuk mengurangi kemungkinan kesalahan dan meningkatkan kenyamanan pengguna. Secara keseluruhan, ECC terbukti menjadi solusi yang aman dan efisien untuk aplikasi berbasis web yang membutuhkan pengelolaan data yang aman di era digital.

## REFERENSI

Alfatah, D., Asimetris, K., & Data, K. (n.d.). *Use Of Asymmetric Cryptography In Securing IOT Communication*. *3*(1), 19–24.

Azlin, Musadat, F., & Nur, J. (2018). Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64. *Jurnal Informatika*, *7*(2), 1–5.

Husaini, F., Pardede, A. M. H., & Gultom, I. (2022). Penerapan Enkripsi Menggunakan Metode Elgamal guna Meningkatkan Keamanan Data Text dan Gambar. *JUKI : Jurnal Komputer Dan Informatika*, *4*(1), 67–73.

Indriyani, T., Dinasti Airlangga, P., Jaka, F., Adhi, I. T., & Surabaya, T. (2023). Enkripsi Data Dengan Mengunakan Metode ECC (Elliptic Curve Cryptography). *Seminar Nasional Sains Dan Teknologi Terapan*, *XI*, 1–9. https://ejurnal.itats.ac.id/sntekpan/article/view/5225/0

Nugroho, Y., & Painem, P. (2022). Implementasi Algoritma Elliptic Curve Cryptography (ECC) Untuk Pengamanan File Berbasis Web. *Prosiding Seminar Nasional …*, *September*, 258–267. http://senafti.budiluhur.ac.id/index.php/senafti/article/view/215

Perdana, D., Purwiko, P., Dewanta, F., & Afianti, F. (2022). *Analisa Penggunaan Elliptic Curve Cryptography pada Sistem Autentikasi pada Internet of Things*. *8*(1), 42–49.

Taopan, G. I., Boru, M., & Fanggidae, A. (2022). Pengamanan Portable Document Format (PDF) Menggunakan Algoritma Kriptografi Kurva Eliptik. *Jurnal Komputer Dan Informatika*, *10*(1), 47–54. https://doi.org/10.35508/jicon.v10i1.5296