KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 2, April (2024), pp. 696-705

Perbandingan Performa dari Algoritma AES dan RSA dalam Keamanan Transaksi

Ahmad Miftah Fajrin[1], Christoper Kelvin[2], Brian Owen[3], Bayu Aji[4]*
[1,2,3,4]Universitas Surabaya, Indonesia
E-mail: ahmadmiftah@staff.ubaya.ac.id[1], s160420021@student.ubaya.ac.id[2], s160420027@student.ubaya.ac.id[3], s160420081@student.ubaya.ac.id[4]

Abstract

Online transactions have become increasingly prevalent in the modern day. It is highly user-friendly and can be conveniently transported to any location. Nevertheless, internet transactions possess inherent security vulnerabilities that render them susceptible to assaults, hence enabling the retrieval of consumers' personal data. Hence, it is imperative to use encryption measures for safeguarding users' personal data, including PINs, CVVs, and card numbers. This study aims to evaluate and contrast the efficacy of AES and RSA algorithms within a website platform designed for online transactions. The study's findings indicate that there is minimal disparity in the performance of the two algorithms. However, it was observed that both algorithms exhibit enhanced security when employing longer keys.

.

Keywords: *online transaction, security, RSA, AES, encryption*

Abstrak

Transaksi online merupakan sebuah metode transaksi yang sangat populer dalam era sekarang. Penggunaannya yang sangat mudah dan dapat dibawa kemana-mana dengan mudah. Namun, transaksi online memiliki kekurangan pada segi keamanan, dimana transaksi ini rentan untuk diserang sehingga data-data pribadi pengguna dapat diambil.. Oleh karena itu sangat penting untuk menerapkan enkripsi pada data-data pribadi pengguna seperti pin, cvv, dan nomor kartu. Pada penelitian ini akan dibandingkan performa dari algoritma AES dan RSA dalam sebuah platform website untuk transaksi online. Berdasarkan hasil penelitian didapatkan bahwa kedua algoritma memiliki performa yang tidak jauh berbeda, dimana keduanya akan memiliki tingkat keamanan yang lebih tinggi apabila kunci yang digunakan lebih panjang.

Kata Kunci: *transaksi online, keamanan, RSA, AES, enkripsi*

1. Pendahuluan

Transaksi *online* merupakan transaksi yang melibatkan alat elektronik seperti kartu debit, kartu kredit, bahkan teknologi yang baru hadir seperti QRIS dimana pengguna *scan* atau memindai kode *barcode.* Kehadiran teknologi dalam bertransaksi sangat memudahkan dan mempersingkat waktu. Akan tetapi, ini dapat menjadi celah keamanan bagi pengguna dalam keamanan dan autentikasi data pribadi. Serangan siber menjadi ancaman yang cukup serius bagi pengguna maupun penyedia layanan transaksi *online*.

Serangan siber merupakan serangan yang mengacu pada finansial, bahkan target militer dan tujuan politik dengan tujuan untuk kepentingan pribadi atau suatu kelompok [1]. Metode serangan umumnya menggunakan serangan virus, *data distribution service* (DDS), *hacking* dan serangan lainnya [1]. Salah satu serangan yang umum di dunia *online* adalah *data tampering. Data tampering* adalah salah satu bentuk kejahatan siber dimana oknum memodifikasi dokumen pengguna untuk tujuan tertentu yang dapat menurunkan kepercayaan pengguna terhadap suatu bank [2].

ISSN: 2720-992X

Pengamanan data sangat diperlukan untuk melindungi segala data pengguna dan mencegah ada nya serangan sekuriti. Data bisa berupa nomor kartu, saldo pengguna, dokumen rahasia, dan masih banyak lagi. Untuk mencegah hal ini, berbagai macam metode enkripsi diaplikasikan guna mencegah terjadinya serangan siber dalam transaksi *online*. Penelitian kali ini akan meneliti pada metode RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) untuk transaksi.

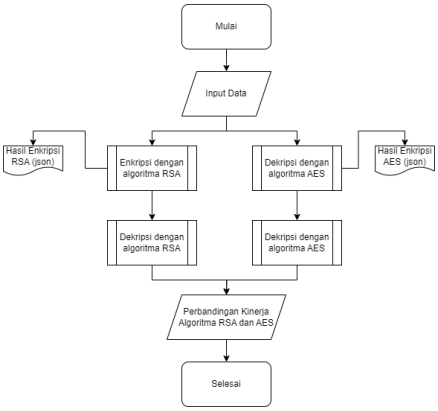
RSA merupakan metode asimetris yang membutuhkan *public key* untuk *encryption* dan *private key* untuk *decryption* [3]. RSA akan memproses tulisan dan mengubah ke bentuk desimal berdasarkan kode ASCII terlebih dulu. Pengubahan ini bertujuan untuk mempermudah perkalian berdasarkan rumus matematis. Proses enkripsi bergantung pada banyak teks dan panjang kunci yang akan di enkripsi.

Pada proses enkripsi, *public key* dan *signature* berperan sebagai autentikasi serta kerahasiaan data [4]. Pada saat pemrosesan, algoritma akan menghasilkan *public key* untuk enkripsi dan diketahui secara massal serta *private key* untuk dekripsi dan bersifat rahasia. *Signature* digunakan sebagai proses autentikasi apakah pesan diterima ke orang yang dituju pada saat dekripsi [4]. Keamanan RSA sangat bergantung pada panjang *key* yang diberi.

AES merupakan metode simetris menggunakan algoritma *Rijndael* yang mampu mengenkripsi dan mendekripsi data dengan panjang 128 bits dan *key* 128 bits [5]. Panjang *key* bermacam-macam mulai dari 128, 192, dan 256 bits. Proses enkripsi pada AES dikenal sebagai *round* yaitu proses merubah posisi kolom matriks dengan cara transpos, subtitusi, dan menggabungkan agar meningkat keamanan [6]. Semakin panjang *key* yang dihasilkan, proses *round* juga semakin panjang. Baik RSA maupun AES merupakan dua metode dengan cara kerja dan keunggulan yang berbeda. Penelitian ini akan berfokus membandingkan cara kerja kedua metode ini. Data yang akan di enkripsi adalah nomor kartu, nama pengguna, serta nomor cvv kartu. Untuk itu, penelitian ini akan membandingkan mana metode yang cepat serta aman dalam melindungi data pribadi pengguna.

2. Metodologi Penelitian

Pada Gambar 1 menujukkan bahwa enkripsi dilakukan pada data pembelian barang, nama, alamat email, nomor hp pembeli, alamat, nomor kartu kredit, nomor cvv kartu kredit, dan tanggal kartu kredit pembeli. Algoritma pengamanan data yang digunakan yaitu algoritma RSA dan AES. Masing-masing algoritma akan melakukan enkripsi dan dekripsi menggunakan input data yang sudah disediakan. Setelah dilakukan enkripsi yang nanti akan menghasilkan json, hasilnya akan disimpan dan siap untuk dilakukan dekripsi. Kemudian dua algoritma akan dibandingkan performanya. Perbandingan dilakukan pada aplikasi berbasis website untuk melakukan transaksi.



Gambar 1. Rancangan Penilitian

2.1. *Cryptography*

Cryptography adalah bidang yang mempelajari metode matematika yang berkaitan dengan elemen keamanan data, seperti *confidentiality*, *non-repudiation*, *integrity*, dan *authentication* [8]. Prinsip cryptography harus memiliki empat kriteria, yaitu data intergrity untuk memastikan bahwa data tidak termodifikasi, confidentiality untuk memastikan data tetap rahasia, authentication untuk memastikan bahwa data dapat diakses oleh orang yang berhak atas akses tersebut dan non-repudiaiton untuk [9].

2.2. AES

AES merupakan sebuah teknik enkripsi yang paling sering digunakan karena efisien dan juga simple. AES adalah sebuah blok *cypher* asimetrik dengan memiliki kunci yang sama untuk *encryption* dan *decryption* [10]. AES diciptakan untuk mengatasi kekurangan-kekurangan pada algoritma kriptografi yang sudah ada seperti DES. DES memiliki kekurangan pada segi *hardware* dan juga *key* yang pendek[5].

Algoritma AES diawali dengan proses pembentukan *key*. Untuk panjang kunci dalam bentuk bytes dapat ditentukan oleh pengguna menggunakan parameter yang ditentukan. Data akan dienkripsi dengan kunci yang telah dibuat. Proses pengamanan data AES menggunakan library *PyCryptodome* dan bahasa pemrograman python dalam pengimplementasiannya. *Pseudocode* dapat dilihat pada Gambar 2.

```
def aes(card_num):
  generateRandomBytes(16)
  createChiperUsingAes with Mode_EAX
  encryptionproses with card_num input
return cipher with nonce
```

Gambar 2. Pseudocode AES

2.3. RSA

RSA adalah sebuah algoritma kriptografi asimetrik yang menggunakan dua kunci yaitu *public key* untuk digunakan pada enkripsi dan *private key* akan dimanfaatkan untuk proses dekripsi [3]. RSA aman karena ketidakmampuan manusia dalam memfaktorkan bilangan bulat yang besar secara efektif [11]. Pernyataan tersebut didukung oleh pernyataan Milanov dimana belum pernah diketahui adanya percobaan pembobolan enkripsi RSA yang berhasil, hal ini dipengaruhi oleh susahnya memfaktorkan bilangan bulat yang besar [12].

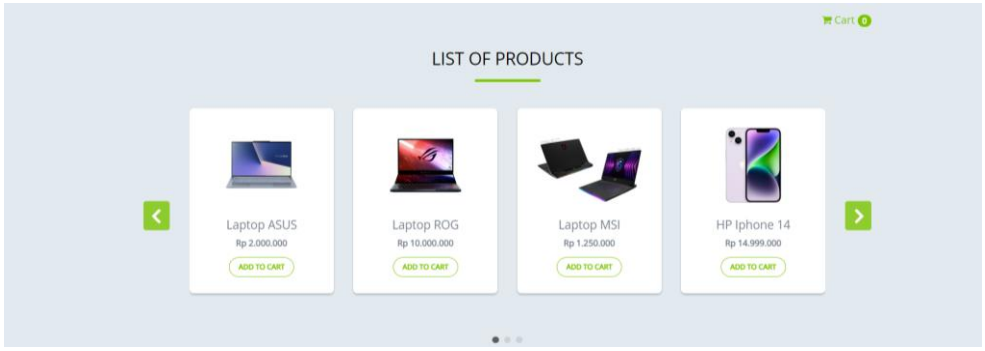
Algoritma RSA diawali dengan proses pembentukan *public key* dan *private key*. Untuk panjang kunci dapat ditentukan oleh pengguna menggunakan parameter yang ditentukan. Data yang akan dienkripsi akan diencode terlebih dahulu lalu dienkripsi dengan *public key*. Proses pengamanan data RSA menggunakan library *rsa* dan bahasa pemrograman python dalam pengimplementasiannya. Potongan kode dapat dilihat pada Gambar 3.

```
1.  from Crypto.PublicKey import RSA
2.  from Crypto.Cipher import PKCS1_OAEP
3.  # Generate RSA key pair
4.  key = RSA.generate(1024)
5.  # Get public and private keys
6.  public_key = key.publickey()
7.  private_key = key.export_key()
8.  # Encrypt and decrypt using RSA keys
9.  def encrypt(message, public_key):
10.     cipher = PKCS1_OAEP.new(public_key)
11.     encrypted_message =
    cipher.encrypt(message.encode())
12.     return encrypted_message
13. # Example usage
14. message_to_encrypt = "1234123412341234"
15. start_time = time.time()
16. encrypted_message =
    encrypt(message_to_encrypt, public_key)
17. end_time = time.time()
18. ex_time_rsa = end_time - start_time
19. print("Execution time: ",ex_time_rsa, "
    second")
20. print(f"Encrypted message:
    {encrypted_message}")
```

Gambar 3. *Pseudocode* RSA

3. Hasil dan Pembahasan

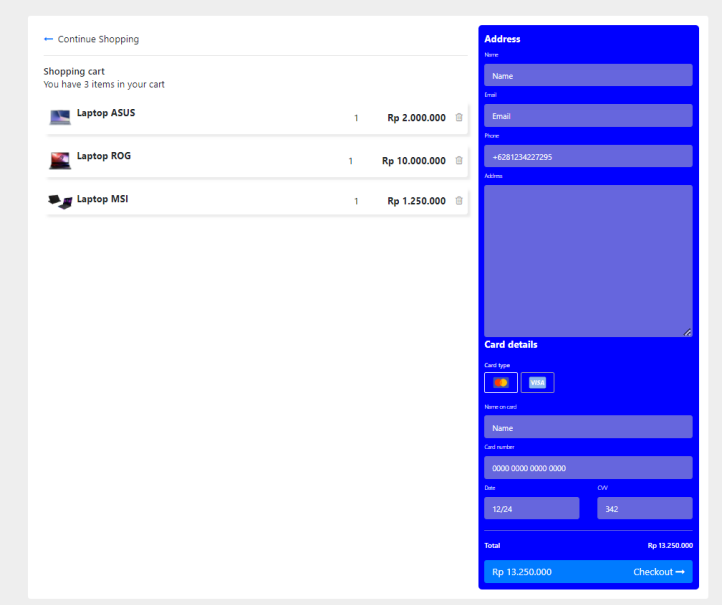
Pengujian dilakukan untuk membandingkan performa terhadap dua algoritma yaitu AES dan RSA. Perbandingan tersebut dilakukan pada sebuah Website yang dapat melakukan transaksi. Untuk tampilan *dashboard* dapat dilihat pada Gambar 4.



Gambar 4. *Dashboard List of Products*

Pada tampilan awal sistem, memberikan sebuah daftar barang yang dijual. Setiap barang ditampilkan gambar barang, harga barang, dan tombol untuk menambahkan barang ke dalam keranjang. Pengguna dapat memilih barang yang ingin melakukan pembelian kemudian akan dimasukkan ke keranjang. Untuk tampilan keranjang dapat dilihat pada Gambar 5.

Pada tampilan keranjang, ditampilkan daftar barang yang telah dimasukkan ke dalam keranjang beserta jumlah dan total harga. Terdapat tombol hapus untuk menghapus barang pada keranjang. Pengguna diminta untuk mengisi data diri seperti nama, email, nomor telepon, dan alamat pembeli. Sistem hanya menerima pembayaran menggunakan kartu kredit sehingga pengguna diharuskan menginputkan jenis kartu, nomor kartu, tanggal *expired* kartu, dan nomor cvv kartu. Apabila tombol checkout ditekan maka pemesanan pengguna akan disimpan dan ditampilkan sebuah tampilan bahwa order telah berhasil. Gambar 5 merupakan tampilan keranjang.



Gambar 5. Halaman Keranjang.

```
"dataAES": {
  "name": b"\xcf\xee\xd1,\xce\x1f\xff\xd9\xdbN\xff\x04\xe1\xad,\xdb",
  "email": b"\x15\xe4N\x8d\xf6\x9a\xd4\xd6\x01U\xb8:\x86\x8as\x18",
  "phone":b"O#\x07\xaf\xf8zp\xc5p\xcf \x96\x98cc\xf7",
  "address": b"\x82\xaeX\xab\xed#fg\x10FD\x7fL\x15m\x80",
  "card": b"\xf6KLNO\xf5\xa9X\xd8N`\xfd'\x8bI$",
  "namakartu": b"\\\x1b\xb6\xef&\x8a\xdc\xf5\xa1,Q\x93\xf9\xd2\xbfJ",
  "nomorkartu": b"/\xf5%OI\xca\x9e\xe3n\xf1\xf1\x88\xda>\x1f\xd2",
  "tanggalkartu": b"\xf3^\x86\xdc\xc9C\xb8\x9e\x86i&!\xaf[\xa8\x17",
  "cvvkartu": b"f\xd7\xb3]\xf9\xcbm\xff\x96\xf2\x88\xa7K\x02+\x0b",
}
```

Gambar 6. Hasil Enkripsi Data Pribadi Menggunakan AES

Pada Gambar 6 menunjukkan hasil enkripsi menggunakan AES untuk data pribadi pembeli. Data pribadi pembeli akan lebih aman jika data aslinya yang tersimpan di dalam database berupa hasil enkripsi.

```
"pembelianAES": [
      {
        "gambar": b"\x8b\xc9A\xd2\x97P\x88b\x9b\xff\xc1\xe7P\x01\xb6Q",
        "harga": b"\x96\xa3q\xde\xe9\xf4\x17\xe9\xf6\x17<>D\xec\xad`",
        "id": b"\x91?\x90\xbd{g\xde\xf4\xde=w\xba\xddJ\x90\xb0",
        "nama": b"\xc4\xae\xc9\x84\xbf(\xf8O\x81\x8b\xd3\xd1h\x89\xe53",
      },
      {
        "gambar": b"\xce }\xe0\xa4\xcb\xbeo!u\x0ca\x10\xb8\xa1\xff",
        "harga": b"\xf47E.\x9e\x01\\\xa5\n\xb4\xd4\xd9\xfeb\x92\xde",
        "id": b"\x99V\xb0\nO\xfe9|\x81\x1a\x16\xad\xdf\x15<\xa5",
        "nama": b"\x9eom\xe3\x95\x02\xb6\xf2\xb0\xc1\xdb\xf3\xaa\x87)\xa9",
      },
  ]
```

Gambar 7. Hasil Enkripsi Pembelian menggunakan AES

Pada Gambar 7 menunjukkan hasil enkripsi menggunakan AES untuk data hasil barang dibeli oleh pembeli. Data pembelian juga diamankan menggunakan AES agar data aslinya tidak mudah dibaca meskipun data tersimpan di dalam database.

Tabel 1. Hasil Uji coba Enkripsi Pembelian menggunakan Algoritma AES

Panjang Kunci (bytes)	Mode	Waktu Eksekusi (s)
16	ECB	0,00015
16	CBC	0,00013
16	EAX	0,00067
32	ECB	0,00018
32	CBC	0,00016

Berdasarkan Tabel 1 didapatkan Panjang kunci diukur dalam bit, mode dan waktu eksekusi. Semakin panjang kunci, semakin sulit untuk melakukan serangan terhadap sistem kriptografi. Pada mode ECB dan CBC, semakin Panjang kunci, semakin lama proses eksekusinya. Ini terkecuali jika menggunakan mode EAX yang membutuhkan waktu lebih lama dari mode lainnya meskipun menggunakan kunci 16 bytes.

'dataRSA':
{'name':b'No\x82\x98\x96\x00fG[\x02`^\xd9~\xae\xdd\xe9\xa3\xe2[\rZ\xa8^\xa1OG\x9a\xba\xe9\x0cs\xfd\xcb\xf2\xcdb\xc9U\x11\x11o\xfe\xb2\xe0\x84o\xc3\xc44oY\xb6\xc7\xc1X"\xd6\xf2\x08.t\xcb\x1a\xbdo7\x9012>M\xc8\xac\xd5\x9a\x1e\xe1tn\xa3g\x04\x1e\xad\xc4\x13\xbe\x91\x8a\xf2\xe9\xd39[\xc7\xeb{Gx\xd7\xd8Ug\xe84d\x06J/!cT\x05\xe8\xff/\xb2W\xc6n\xfd\xae\xfc7m\xff]',
'email': b'l\xed:\xc4\x84\xb2\x8fe\xc8\xe6\xd10d\xe3\xae\xc4\x15c+\xcd%\xab\x95\xb7\xf9]q%\x90\x97\xdd\xe8\xe0\x87Vc\x10\x18$\xf8\x0f\x9fr\xb2\x15\xb5\xbd\xe8N\xa9\x97\xba\xbbD)$\x13\xfbo\x9d\xf3\x83\xbeUJ\xa9\x1c\xb2L|t\xf8\xeao\xffh\xa1\x91\xf0\x1f\xab\xcch\x01\x1b\xdcw7\xcee\x1e\xe1R/U\x10n\xde\x00B\xff\x84\xed\xad\xb4,H\x9f\x8e\xb5\x8a\x8d\xdd\x90\x8dS|\xe6\xb7\xe2\xd8\x00Ri\x00\x86n',
'phone': b'Mu\x92\xdf\xb5\xa63\xd3\xc7F\xe8\xcb\x9c\x9f\x0eky}?\xd7JN\x04\xe6\xaa\xca\xce\xa0\x06O\x15\x00\xc4\xffr\xcf\xc2\x88\xc14\xceJ\xdd;V\x00\xa8\x89"c\x88F\xc7\xa1\xdf!\xf5\xa8\x85\x1c\x17\xb04q\x93\xce\xc1\xfb\xc1kN\x03p>\x96\xc3\xcaDs\x1asz\xb6>AoY\xc6\x1c\x07=z1\xd5\xac\xd2\x89\x080ni\xe6\xd3\n\xfb\x1f\xed\xb6\xb1\x96\x0e\xe5\x8f\xc0\x0b`\x8b\xac\xfe\xce\xc9\xe4hynr',
'address': b"Ty<V\xce\xd7bv\x0ff\xb0\xb1aq\x01\xd5\xf6\xc0\xb6\x8e\x88*\x08\xcf\xb5\xba\x8f\x97\xa7G\xe7\xf4x\xf9x23:\x1f\x1dM\xd7C\xb1EB#\xb7\x009\xa8\xadQ\xea\xfds\x90+'d\xd4\x13\xb0s\xba\xcaM7\xe9p\x91\xf5\x08C!.\x81\x1bF\x91\x89a\xbam\x9a/\x97\xe8\xd4\xd9\xb7_\x06.\xf0\x0fn\x91\xb14J\x83A*\xea\xf1\xc47OO7\xc3\xb0\xb7\xb4\xf1\xa4\x93\xec\x8a\xba\xc5\x97h]\xad\xe7\xa1", 'card': b'S\xcb\x1b\x8b\xadE\x02\xe2H<\x1d\x11X\x98ONdM\xe4t\xe8\xf4\xa6\xca`\xcc\xc5.\xdd\x08\t\x17\xb4_\xea6\x9b\xf2\x16b\x8f\xd6\x15\xc0\x8a@k\x0f\xe2\xb7\x1fsPaX(Tn\xb8\x1eS\xf0\"\x15\xf9\x9bq.\xb5\x86{+\xe9\xb1\xdf\xa1\xe4\xe3\x13D\xbf{h\xe4\x89\x03\xb2\xc5,-\xc5\xdf\xc2\xf5\x1ag\xc2\'8\xe3\x07Ve\x8a\x99\x19\xe7\xa5i\xd6~\x98\xc5X\x13z\x19\x1e$\x19\xec]d\x9f\x88\x97"e',
'namakartu': b'\x04\xbb\x8aa\xbb\xcd\xd2D|\x06\xe9\xbf\x1e\\\xae$\x86(\x94\x9c\xb6\xf8%my1\x00\x8d\x1dx.\xca\x19R]\x9b\x99p\x82\x9f\xb4\xb7\x8b\xa4^y\x90d\xb1\x8e/:\x97\x02.\\\x18\x01\x83\xf7\xa2\xc5\xfa\xff\xa1\x85m^4f\t\x1b\x99wb+i5\x1b\x1a\xe5\x9c\xe4md\xf4\xe4\xdc\xe6\xf7\xa2\xb2\xc6\xf0S\xb5\xa8\xc3h\xd0f\x17\n\xdd\xcf\tr\xb6B\xb1\xfe:,\xf4ib\x85\xe0\x9b@\x03*\xd8,\x05\x0f\xd9\x1d',
'nomorkartu': b"c[\x17\x9b;*\x00$E\xa6\x14h\\c\xc6!\x86\x83\x1fU\x02X<\\\x8f0\xab\xdb\x05\x8a\x80)~\x86\xe2\xfe4\x13gpu9cm{\\\xa2_M\xea`|\xad@\x0b-\x878\xc6\xf1@\x94\xb6\xc2H\x93\x8f\xb6\xd1j\xe3\xf2c\xcf}=x+,\xf7\xbcq\x05\"\x87\xc5)\xddfo\xbe\x08\x82\x8dBq\x8e\xd3]\xe7G\xc8\x08\xeb\xbc(F\x1c\x1c\xd0`\x88\x11\xc7\x9e\\\xe0?\xde\x02S\x8bMv\xad\x15\xba\xb6",
'tanggalkartu': b"1\xe4a\xa1\xf4\xac\x9eBY\x9e\x8d\xa4pd^\xfa\xbc\ra\xa12\xdb\x1avJ\x01\\`Z\x92G(\xacdf\x89\x0e6\xbc5\xac\xcd\x83\xd8\xf5\xe6\xf5\\\xd5\x0c\x85\xa2\x8aW\xce\x05\xe0\xd3\xb65\x17"\x92\xeb^\\)\x9cq\xed4:\xf72)\xa3\x8d\x00\x96\n\x18A\xe8\x176\xa0\xe4{q\x84*\x00\xe8\xcf\xfc,\xaf\xa6H9\xd8\x11#]u|S\x19\xd1T0\xc3\x1f\xd3\xb9HQ\x9a\xba\x1eH{\x19\x93\xc7\x0eLh",
'cvvkartu': b'\x94\x00-\x81@\xc1U\xc7<\x16;\xb1r\x89\x1aG\x82I\xd5\x82\x0cy\xd8<\xd6\x85ZM6\x08\x92\xa8\xe5\xef#\x9e\x9dW\x85(k;AHpC\nog\xa4WP\xd1\xe1\xd1\xc36\xa0=\xe0\x8c_\xda\x95E\r\xbf\x13\xe6^z[\xc0H\xb7\x9f\xeaI\xe3y\xdczA\xf8\xa1R@\xbd\x1a\xf2:\xcaFX!\xab\\$\xcc\xb7\xe5\x92\x9b=\x13\xcb\xbd\xd8\x1d\xdal\xb6]\xaf\x85\x10,\xfd\x11-\xa7UY+y|\n'}

Gambar 8. Hasil Enkripsi Data Pribadi Menggunakan RSA

Pada Gambar 8 menunjukkan hasil enkripsi menggunakan RSA untuk data pribadi pembeli. Data pribadi pembeli akan lebih aman jika data aslinya yang tersimpan di dalam database berupa hasil enkripsi.


```
'pembelianRSA': [
{
  'gambar':
    b'\r\x8a\x8f\xb22\x8b\xb7ZD77\x83Z\x97\x17\xe4\xa8\x87.q7\xf1*\xce\xeb\x9a\xd8\xa1\x9
    8\xdd.\xf9\xba\xcd\xf4K?0\x87\x8c?\x15\x1f_yrY\x97\x81\xa2\xc8\xb4\xa9\xe59\x86G\xd9\
    xa1\x98d\x98C\xe73\x961\xde,\xdf\x89\x12\x10c\x0b\x80\xdc\xe3:\x9d)\xb3\x1bwDR"\x1c
    q\xaa\xc0\xd3\x93K0\x0e\x11tuH\xf4r\x06\xbat\xe4\x19*a\xaf\x7f\xc8\xd4o:\xb7\x9a\xc60
    B\xfb\x82\xf5{<O\xdfi',
  'harga':
    b'^\x9e\xb8_a\x01\xcf1\x08m\x9c:\xb1~\x81\xed\xb7\x80\xd3\x06\xb4t\xe7n)&u\xde\xc1\xa
    5\xde
    Nr\x06\xee\xd6\xd6\x8b\xd8\n!d\x85^\xc4?:\\F\xaf\x119D\x9d\\Xsd\xe2\xb8RU\x1ac\xcb\x0
    3\xf5\xf4"O<\xe5]\xac\x8dp\x0bj\xb7\xa1\xc5\x98iu\x7f.\rg\xc6]\x08A\x1d^\xf0U\x0b\x91\
    xa13\x8a\x89\xa9\xe9\xb1\x8b\xc8\x97\x8b\xf9\xef\xd9x\xa1\x83\x9e\xbb\xf1\x92N\xf4\xc
    b\x9a9q\xca>', 'id':
    b'E\x82,\xc5T\x9e\x9a\xdfD\xcc\xe4\xe7\x8b8x2\xaf\xb4}\x01\x9d\xb5sc,#\x16\x02\xaa\xef
    T\xb1R\xfd$&\xd1+L\xdc\xae\xf94\xb0\x9b\xf0\xb1\xcc\xde\x1b[\x1c\x01,2P\xcf\r\xe3\xae\
    x96\xfd\r5r\xe5\x08/2\x80\xa78\x9d+\x86\x94\x94\xc2\x10^
    ]\x1dB\ra\xf5\xa8\x80\x89R\xf8\xf3E/T>S\x04\x92\x80\xd4\xea\x9am\xb6\xea\xde\xc1p\x0
    bj\xf1\xcb\x90\xa2\xd3\x1em~\xe3Ym\xb9\xd3\xee\xb3Q',
  'nama':
    b'n\x89E\x14\x1f\x03\xa7\xe0\xb5\xa6\xa7\xb8\xedK\xaad\x87\xce\x8cYJ\xe4\xa7\xbc\xbbb
    \xdei\xb7\x9c8\xe6\xb7\x04\\\xce\xff+\x88\x1e\x84D\xa4\x06F\x91x\x97Q&v\xd1\x19\x88\
    xc8\x9b\xc5\xad\xeb\x92t)\xf4\x95\x96\x0fX\xcf@\xc6O\xd6;\xb3\x8b\xdc^6\x00u\xdec\xc
    4\xf5f;s\x87Mo6Kw\xc6\xc1x\x90P\xae.|\xf3R\x86fZ\xab\x0f\xba`\x00\xfb\xc4\xb2\xffT\xc
    1\xba\xd3\xba(Q"(\x10\x0e\xb1\xa3'
},
{
  'gambar':
    b'\x00#\xc7+\x07\xc7\xda\x819Qi6y\x97\xeb\xaeo\x97\xabK\xf4\x93\xc9z\xa2\xc4\xe7i/b\
    xc4\xa4\x0c\x9a:\x1b_\xe2\x14\x85\x1d\xa8\xc4\xe9\xa96&\xf1\xb2\xdf
    #X[\xbe\x08\xe5\x17\xa1\xe2\x7f`\xe4A\x88\x14x\x8b0\xaa\xd9\x08d\x8a\xca\xca\xf8\xb5
    \x99\x8d\x99QC6\x98\x0b\x81-
    ^\xd1Z\xe4\xcf\xa3\x14\x0e\xb3?\xa0~\x9b")k\xa0\x0b#\xda\xdc}\x8a\xa4\x03\x82D\xb7\x
    df ?E\xb5\xc6\x0e\xd5+\x9a\xbcY',
  'harga':
    b"6\x08<\xd1\xd4\x1b\x9e\x18x\xb4>\x90\x023\xbf\xb7\xae\xfa?\xc2\xc4\xb6\x97\x87\x89
    \xdd\xb1Q\xba\xd9\x94\xd1&/\xea\xae\x14K\x858\xa3\xfflg\xee\xdcV|W`\xff\x0c\x8c\xa7\
    x04\xb3\xa9\xc3\x9b\xd6_\x00/'~P=\xc5\xe1@\xe0\x05Y\xd3\x14\x10\xdeB4$\x0f\x91i$n\
    x0bwKh<\x9d\x08\xf2C|?\xca\xb9\x19\xca\x10\xc2\xe8J\xca{\x1bk\xfb\xac\tV\xd9\xeaSv\
    xc4f\xc1\xe2\x91\x96/\x9f\xc3\x17\x1f\xd2", 'id':
    b'P\xbcG\xdf\x0eC\x03\xff\x89\xe2\xc0\x9e\x80\x15\xb6\xfb\xfd*/\x06\x08\x1f\xdf@S\x8
    b\xe2\xa8\xb4\xb8F\xde\xd5b\xf1V\xaf\xa1:\xf9\x15\xf7\xc8\x82E\xbc\xbf\xac&M\xb5\x1
    b\xcbh\xe9\xd0a\xe1\xb7\x88\xa0\xe2\\G%%\x03>\xbe\x18>\x9eU9\xeaH\x82D\\Ik\x86l\x
    cd\xd4\xcb\xc9\x86\xbe\xf5\xaf\xf1V\xbc?\xb9\xef\xaeT>\x93\xe2V\xabB;\x08\x83\x95\xa
    1\xcb<\xbd\xf1r\x00)\xbdD\x84\xe7F[U\xd5\xae\xbb\xa7',
  'nama':
    b'hNlv\x0f\xa5\xa8\xbd\xb7\xa6}\x80\xec\x94\x8a\xa0\xb2mU$\x14\\M\xf8\xb5\x1al\xbd\x
    14\x9d\xbe\xe4!\tI\xdb8AR\x0bV$\x8f\xf1\x7fC\xe8\xa9\xc3\xc9\x91;\xd8I\x06+i~$\xb9\x
    94m%\xe7\xad\xbc\xd1ggZ\x7f[]Cng|\xc1\xfd\xc7\xba\xf5c2,\xe2z\xa3\xf4\xb2\xefYb`f\xe
    5\x15\xc0\xe6&\x98\xb2\x121\x7f"%\x1db\x1dRj\xba;y\xe7\xaf\xcb\xf7\xb8\x9b\xc9\xe2_\
    xae\xcf\xb2\xb5'}]
```


Gambar 9. Hasil Enkripsi Pembelian menggunakan RSA

Pada Gambar 9 menunjukkan hasil enkripsi menggunakan RSA untuk data hasil barang dibeli oleh pembeli. Data pembelian juga diamankan menggunakan RSA agar data aslinya tidak mudah dibaca meskipun data tersimpan di dalam database.

Tabel 2. Hasil Uji coba Enkripsi Pembelian menggunakan Algoritma RSA

Panjang Kunci (bytes)	Waktu Eksekusi (s)
1024	0,000465
2048	0,000861
3072	0,001921

Berdasarkan Tabel 2 didapatkan Panjang kunci diukur dalam bit, dan semakin panjang kunci, semakin sulit untuk melakukan serangan terhadap sistem kriptografi. panjang kunci RSA yang lebih besar memberikan tingkat keamanan yang lebih tinggi, tetapi juga meningkatkan kompleksitas perhitungan. Waktu yang dibutuhkan untuk enkripsi dan dekripsi pesan menggunakan kunci RSA berkorelasi langsung dengan panjang kunci. Semakin panjang kunci, semakin lama waktu yang diperlukan untuk melakukan operasi kriptografi.

Tabel 3. Perbandingan RSA dan AES

Kategori	RSA	AES
Keamanan Data	RSA memperoleh keamanannya dari kesulitan memfaktorkan produk dari dua bilangan prima besar. Semakin besar panjang kunci, semakin sulit bagi penyerang untuk memfaktorkan kunci dan mendekripsi pesan yang dienkripsi dengan RSA. Dalam kondisi normal, RSA dianggap sangat aman jika panjang kunci yang digunakan cukup besar.	AES mengandalkan kekuatan keamanannya pada ketidakmampuan untuk menemukan pola dalam perubahan bit dari data yang dienkripsi. AES telah terbukti sangat kuat dan tahan terhadap berbagai jenis serangan. Kekuatan keamanannya terkait erat dengan panjang kunci yang digunakan, dan panjang kunci yang lebih besar memberikan tingkat keamanan yang lebih tinggi.
Waktu Eksekusi	Proses enkripsi dengan RSA melibatkan eksponensiasi modular, yang bisa menjadi lebih lambat terutama dengan panjang kunci yang besar.	Operasi enkripsi dengan AES lebih cepat dibandingkan dengan algoritma RSA.
Key Management	RSA menggunakan pasangan kunci publik dan pribadi. Manajemen kunci RSA melibatkan pertukaran kunci publik secara aman dan menjaga kerahasiaan kunci pribadi. Manajemen kunci RSA melibatkan pemilihan panjang kunci yang sesuai untuk mencapai tingkat keamanan yang diinginkan	AES menggunakan kunci simetris yang sama untuk enkripsi dan dekripsi. Manajemen kunci AES terkait dengan pertukaran dan penyimpanan kunci simetris secara aman.
Panjang Kunci	Semakin panjang kunci, semakin sulit bagi	Panjang kunci yang umum digunakan adalah 128, 192, atau

Kategori	RSA	AES
	penyerang untuk memecahkan kunci dengan melakukan faktorisasi. Panjang kunci yang umum digunakan adalah 1024 dan 2048	256 bit. Panjang kunci yang lebih besar pada AES memberikan tingkat keamanan yang lebih tinggi.

Berdasarkan Tabel 3, Hubungan antara panjang kunci AES dan waktu yang diperlukan untuk melakukan enkripsi atau dekripsi bergantung pada beberapa faktor, termasuk mode operasi, implementasi perangkat keras atau perangkat lunak yang digunakan, dan kecepatan komputer atau perangkat tersebut. Secara umum, semakin panjang kunci AES, semakin kuat keamanannya, tetapi pada saat yang sama, semakin lama waktu yang dibutuhkan untuk melakukan operasi kriptografi.

Terdapat beberapa perbandingan yang dapat dibahas setelah melakukan percobaan terhadap pengamanan data dengan algoritma RSA dan AES. Tabel 4.3 merupakan tabel perbandingan antara algoritma RSA dan AES berdasarkan keamanan data, kinerja, panjang kunci, dan *key management*.

4. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan pada aplikasi sederhana yang menggambarkan skenario jual beli dengan transaksi *online*. Hasil yang didapatkan bahwa RSA dan AES tidak memiliki perbedaan yang jauh pada tingkat keamanan. Tingkat pengamanan data dari kedua algoritma tergantung pada panjang kunci yang digunakan. Secara waktu eksekusi, AES dapat memberikan waktu eksekusi yang lebih cepat dari pada RSA, dimana RSA membutuhkan waktu yang lebih lama karena adanya perhitungan yang cukup rumit. Untuk implementasi pada pengamanan data transaksi kedua nya dapat disimpulkan memenuhi semua standart umum yang digunakan oleh industri kartu pembayaran.

Saran untuk penelitian selanjutnya yang dapat diberikan adalah pada algoritma enkripsi yang digunakan. Algoritma enkripsi simetrik berdasarkan penelitian yang dilakukan sudah dapat memenuhi standar keamanan kartu pembayaran. Penggunaan algoritma enkripsi lain seperti enkripsi asimetrik diperkirakan dapat memberikan keamanan yang lebih baik dari enkripsi simetrik. Hal tersebut memungkinkan karena enkripsi asimetrik tidak memerlukan kunci dalam melakukan enkripsi dan dekripsi, berbeda dengan enkripsi simetrik yang menggunakan kunci, sehingga ada kemungkinan enkripsi asimetrik dapat memberikan keamanan yang lebih baik dari simetrik

Daftar Pustaka

[1] Li, Y., & Liu, Q. (2021). A Comprehensive Review Study Of Cyber-Attacks And Cyber Security; Emerging Trends And Recent Developments. Energy Reports, 7, 8176–8186. Https://Doi.Org/10.1016/J.Egyr.2021.08.126

[2] Aziz, N., Rodiah, R., & Susanto, H. (2021). Encrypting Of Digital Banking Transaction Records: An Blockchain Cryptography Security Approach. *International Journal Of Computer Applications*, *174*(24), 21–26. Https://Doi.Org/10.5120/Ijca2021921147

[3] Sihotang, H. T., Efendi, S., Zamzami, E. M., & Mawengkang, H. (2020). Design And Implementation Of Rivest Shamir Adleman's (Rsa) Cryptography Algorithm In Text File Data Security. Journal Of Physics: Conference Series, 1641(1). Https://Doi.Org/10.1088/1742-6596/1641/1/012042

[4] Galih, M., & Ramadhan, R. (2021). *Theoretical Mathematics , The Creation Of The Rsa Algorithm , And Breaking It Using Algorithms Based On The Same Idea*.

[5] Muttaqin, K., & Rahmadoni, J. (2020). Analysis And Design Of File Security System Aes (Advanced Encryption Standard) Cryptography Based. *Journal Of Applied Engineering And Technological Science*, *1*(2), 113–123. Https://Doi.Org/10.37385/Jaets.V1i2.78

[6] Guy-Cedric, T. B. I., & R., S. (2018). A Comparative Study On Aes 128 Bit And Aes 256 Bit. International Journal Of Scientific Research In Computer Science And Engineering, 6(4), 30–33. Https://Doi.Org/10.26438/Ijsrcse/V6i4.3033

[7] Ramadhan, P. S., Syahril, M., Kustini, R., Winata, H., & Gea, R. D. (2023). Pengamanan Data Transaksi Menggunakan Aes Dan Rc4. *Journal Of Computer Engineering, System, And Science.*

[8] Hidayat, M. ., Tahir, M. ., Sukriyadi , A. ., Sulton , A., A, C. A. S., & F, . S. A. . Penerapan Kriptografi Caesar Chiper Dalam Pengamanan Data. Jurnal Ilmiah Multidisiplin, 2(03). Https://Doi.Org/10.56127/Jukim.V2i03.619

[9] Barakat, M., Eder, C., & Hanke, T. (2018). *An Introduction To Cryptography*.

[10] Kumar, P., & Rana, S. B. (2015). *Development Of Modified Aes Algorithm For Data Security*. Optik 127. Https://Doi.Org/10.1016/J.Ijleo.2015.11.188.

[11] M. Shand And J. Vuillemin, "Fast Implementations Of Rsa Cryptography," Proceedings Of Ieee 11th Symposium On Computer Arithmetic, Windsor, On, Canada, 1993, Pp. 252-259, Doi: 10.1109/Arith.1993.378085.

[12] Milanov, E. (2009). *The Rsa Algorithm.*