Journal on Education
Volume 06, No. 02, Januari-Februari 2024, pp. 12077-12081
E-ISSN: 2654-5497, P-ISSN: 2655-1365
Website: http://jonedu.org/index.php/joe

Implementasi Keamanan Pesan Teks menggunakan Kombinasi Enkripsi 3Des dan Base64

Andri Purwoko[1], Bambang Suharjo[2], Richardus Eko Indrajit[3], H.A Danang Rimbawa[4]

[1,2,3,4]Universitas Pertahanan Indonesia, Kawasan IPSC Sentul, Kec. Citeureup, Kab. Bogor, Jawa Barat
andri.purwo82@gmail.com

Abstract

Triple DES (Triple Data Encryption Standard) is a symmetric algorithm in cryptography that is used to secure data in the form of text messages by encoding text messages. The processes carried out in encoding the data, namely the encryption process and the decryption process. The triple DES algorithm is a development algorithm from the DES (Data Encryption Standard) algorithm. The difference between DES and triple DES lies in the length of the key used. DES uses one key that is 56 bits long, while triple DES uses three keys that are 168 bits long (each 56 bits long). In this research, the use of 3Des encryption will be combined with Base64 to secure information in the form of text using the Python programming language.
Keywords: Triple DES (Triple Data Encryption Standard), Encryption and decryption, Cryptography, Base64, Security of text information.

Abstrak

Triple DES (Triple Data Encryption Standard) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data berupa pesan teks dengan cara menyandikan pesan teks. Proses yang dilakukan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Algoritma triple DES adalah suatu algoritma pengembangan dari algoritma DES (Data Encryption Standard). Perbedaan DES dengan triple DES terletak pada panjangnya kunci yang digunakan. Pada DES menggunakan satu kunci yang panjangnya 56-bit, sedangkan pada triple DES menggunakan tiga kunci yang panjangnya 168-bit (masing- masing panjangnya 56 bit). Pada penelitian ini penggunaan enkripsi 3Des akan dikombinasikan dengan Base64 untuk mengamankan informasi berupa teks dengan Bahasa pemograman Python.
Keywords: Triple DES (*Triple Data Encryption Standard*), Enkripsi dan dekripsi, Kriptografi, Base64, Pengamanan informasi teks.

✉Corresponding author: Andri Purwoko
Email Address: andri.purwo82@gmail.com (Kawasan IPSC Sentul, Kec. Citeureup, Kab. Bogor, Jawa Barat)
Received 28 December 2024, Accepted 3 January 2024, Published 11 January 2024

PENDAHULUAN

Pada era digital saat ini keamanan pada sebuah informasi sangat dibutuhkan. Dengan semakin banyaknya informasi yang disimpan maka semakin besar pula resiko pencurian data. Salah satu solusi untuk mengatasi permasalahan ini adalah dengan menerapkan teknik Kriptografi (cryptography) berasal dari bahasa Yunani: “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Jadi, kriptografi berarti “secret writing” (tulisan rahasia). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Rinaldi Munir, 2006). Namun pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi, pengertian kriptografi modern adalah tidak saja berurusan dengan penyembunyian pesan, namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Rifki Sadikin, 2012).

Salah satu metode kriptografi yang akan dipilih pada penelitian ini adalah 3Des. Varian ini

umum dikenal sebagai mode EEE (untuk enkripsi) karena pada proses enkripsi semuanya menggunakan enkripsi. Untuk menyederhanakan interoperabiliy antara DES dan 3DES, maka langkah ditengah (pada proses enkripsi 3DES) diganti dengan dekripsi (mode EDE). Dengan pengubahan ini, maka dibuat beberapa versi 3DES. Versi pertama 3DES menggunakan 2 buah kunci, K1 dan K2 (Rinaldi Munir, 2006). 3Des ini akan dikombinasikan dengan Base64. 3DES (Triple Data Encryption Standard) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan suatu data berupa pesan teks. Proses yang dilakukan dalam penyandian pesan teksnya, yaitu proses enkripsi dan proses dekripsi, prosesnya adalah mengulang algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih. Algoritma triple DES termasuk kedalam kriptografi modern, karena penyandian modern berorientasi pada mode bit.

Kriptografi memiliki peran penting dalam menjaga keamanan informasi di era digital saat ini, terutama dalam mengamankan data sensitif seperti informasi keuangan, medis, dan militer. Dalam pengembangan teknologi informasi, kriptografi juga digunakan dalam berbagai aplikasi seperti e-commerce, internet banking, dan layanan pesan instan yang menjamin privasi pengguna.

Python merupakan bahasa pemrograman tingkat tinggi yang didesain untuk memudahkan penulisan kode dan membaca sintaks yang lebih mudah dipahami manusia. Bahasa ini dikembangkan pada tahun 1990 oleh Guido van Rossum dan menjadi salah satu bahasa pemrograman yang populer di seluruh dunia. Python memiliki banyak kelebihan yang menjadikannya salah satu bahasa pemrograman paling populer saat ini. Salah satu kelebihan utama Python adalah mudah dipelajari dan dipahami. Sintaks Python yang sederhana dan mudah dibaca memungkinkan pemula untuk belajar dan memulai pemrograman dengan cepat.Python juga sangat fleksibel dan mudah diintegrasikan dengan berbagai platform dan sistem operasi, sehingga pengembang dapat menggunakan bahasa pemrograman ini untuk mengembangkan berbagai jenis aplikasi, mulai dari desktop, web, hingga aplikasi mobile.Kelebihan lainnya dari Python adalah adanya ribuan library dan modul yang tersedia secara gratis, seperti NumPy, Pandas, dan TensorFlow, yang memudahkan pengembang untuk membangun aplikasi atau solusi perangkat lunak dengan cepat dan efisien. Selain itu, Python juga memiliki dukungan komunitas yang kuat dan aktif, sehingga pengembang dapat dengan mudah mencari bantuan dan memperoleh solusi atas berbagai masalah yang muncul dalam pengembangan aplikasi.

Dalam industri, Python juga banyak digunakan untuk pengembangan aplikasi kecerdasan buatan (AI) dan pembelajaran mesin (machine learning), karena kemampuan Python dalam memproses data dan mudah digunakan dalam lingkungan pengembangan AI. Semua kelebihan ini menjadikan Python sebagai pilihan yang sangat baik bagi pengembang dan organisasi yang mencari bahasa pemrograman yang fleksibel, mudah dipelajari, dan kuat. Berdasarkan latar belakang diatas penulis memiliki ide untuk melakukan implementasi mengenai teknik enkripsi dan dekripsi pesan teks menggunakan kombinasi 3DES dan Base64.

METODE

Untuk melakukan penelitian mengenai Implementasi Enkripsi dan Dekripsi menggunakan kombinasi Enkripsi 3Des dan base64 dibutuhkan kebutuhan sistem secara hardware maupun software. Pada tabel 1 menampilkan kebutuhan hardware dan software yang dibutuhkan dalam penelitian ini.

Tabel 1. Kebutuhan Software dan Hardware

Kebutuhan Hardware	Kebutuhan Software
Intel Core i3-6006u	Pycharm
RAM 4GB	Python
SSD 512GB	Library Pycryptodome

Untuk melakukan penelitian mengenai Implementasi Enkripsi dan Dekripsi menggunakan kombinasi Enkripsi 3Des dan base64 dibutuhkan kebutuhan sistem secara hardware maupun software. Pada tabel 1 menampilkan kebutuhan hardware dan software yang dibutuhkan dalam penelitian ini.

HASIL DAN DISKUSI

Standart DES

DES beroperasi pada ukuran blok 64-bit. DES mengenkripsikan 64-bit plainteks menjadi 64-bit cipherteks dengan menggunakan 56-bit kunci internal yang dibangkitkan dari kunci eksternal yang panjangnya 64-bit.

Proses Enkripsi dan Dekripsi

Berikut alur enkripsi dan dekripsi pada penelitian ini :

1. Menentukan tiga kunci yang akan digunakan untuk mengenkripsi data. Setiap kunci harus memiliki panjang 56 bit.
2. Membagi pesan yang ingin dienkripsi menjadi blok-blok dengan panjang 64 bit.

Proses enkripsi dilakukan sebanyak tiga kali, dengan menggunakan tiga kunci yang berbeda-beda pada setiap tahap enkripsi. Proses enkripsi dilakukan dengan cara mengirimkan blok pesan yang telah dibagi tadi melalui beberapa tahap yang terdiri dari substitusi, permutasi, dan operasi bitwise. Hasil akhir dari enkripsi ini adalah pesan yang telah dienkripsi dengan 3 kunci yang berbeda.

Setelah proses enkripsi 3DES selesai, pesan hasil enkripsi dapat dikirimkan ke tahap berikutnya yaitu tahap enkripsi Base64. Konversi pesan hasil enkripsi 3DES ke dalam bentuk biner.

3. Memecah pesan biner menjadi blok-blok dengan panjang 6 bit.
4. Setiap blok biner diubah ke dalam bentuk bilangan desimal.
5. Konversi bilangan desimal menjadi karakter ASCII menggunakan tabel karakter Base64.
6. Gabungkan karakter ASCII yang dihasilkan dari setiap blok biner menjadi pesan yang sudah dienkripsi menggunakan kombinasi 3DES dan Base64.

Implementasi Program

Pada gambar 1 menampilkan cuplikan code untuk melakukan enkripsi informasi teks. Hasil enkripsi 3Des akan di lanjutkan proses enkripsi base64.

```
def encrypt(plaintext, key):
    plaintext = pad(plaintext)
    cipher = DES3.new(key.encode(), DES3.MODE_ECB)
    ciphertext = cipher.encrypt(plaintext.encode('utf-8'))
    ciphertext = base64.b64encode(ciphertext)
    return ciphertext.decode('utf-8')
```

Gambar 1. Code Enkripsi 3Des dan Base64

Pada gambar 2 menampilkan cuplikan code untuk melakukan dekripsi informasi teks.

```
def decrypt(ciphertext, key):
    text = base64.b64decode(ciphertext)
    cipher = DES3.new(key.encode(), DES3.MODE_ECB)
    s = cipher.decrypt(text)
    s = unpad(s)
    return s.decode('utf-8')
```

Gambar 2. Code Dekripsi 3Des dan Base64

Pada gambar 3 menampilkan hasil implementasi Kombinasi Enkripsi 3Des dan Base 64 menggunakan Bahasa pemograman python dan gambar 2 menampilkan hasil dekripsi pesan yang telah dienkripsi.

```
Pesan: Halo ini dienkripsi kombinasi 3Des dan base64
mkmnL57qzacXi2VPlT422urMHXosóq3GGW1+vWOuMhBDPPjCiYc/0ifkU1WyE9j7
```

Gambar 3 menampilkan hasil dekripsi menggunakan pemograman python

```
Pesan: Halo ini dienkripsi kombinasi 3Des dan base64
mkmnL57qzacXi2VPlT422urMHXosóq3GGW1+vWOuMhBDPPjCiYc/0ifkU1WyE9j7
```

Gambar 4 menampilkan hasil dekripsi menggunakan pemograman python

KESIMPULAN

Proses enkripsi dan dekripsi suatu data dengan algoritma 3DES dilakukan dengan cara mengimplementasikan algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih. Diharapkan Implementasi Kombinasi algoritma triple DES dan Base64 ini dapat menjadi alternatif metode enkripsi / dekripsi dengan algoritma lain seperti algoritma AES dan RSA, agar isi pesan teks asli lebih sulit diketahui orang-orang yang tidak berkepentingan.

REFERENSI

M. Abid and A. Ahmad, "Triple Data Encryption Standard (3DES) for Data Security in Internet of Things (IoT)," in IEEE Access, vol. 9, pp. 7319-7334, 2021.

N. Ahmed, H. Khan and A. Alghamdi, "Hybrid Algorithm for Secure Data Transmission using 3DES and RSA Encryption," in IEEE Access, vol. 9, pp. 140464-140480, 2021.

S. S. S. Mohd Rosli, S. A. R. Al-Haddad and S. K. M. Kamaruddin, "Design and Analysis of 3DES and RSA Cryptography in Data Communication," in IEEE Access, vol. 9, pp. 128689-128702, 2021.

R. M. Al-Zoubi, M. A. Awajan and Y. M. Al-Smadi, "Implementing and Evaluating the Performance

of 3DES Encryption Algorithm using Cloud Computing Environment," in IEEE Access, vol. 10, pp. 12532-12543, 2022.

Z. Zhang, Q. Lu, Y. Dong and J. Li, "Efficient FPGA Implementation of 3DES Algorithm Based on an Optimized Architecture," in IEEE Access, vol. 10, pp. 10551-10563, 2022.

M. A. Rahman, A. B. M. A. Awwal and A. M. A. H. Akhand, "Enhancing Security of 3DES Algorithm by Changing Key Length," in IEEE Access, vol. 9, pp. 89717-89724, 2021.

J. Wang, Y. Wu and Y. Wu, "Optimizing 3DES Encryption Based on Parallel Computing and GPU Acceleration," in IEEE Access, vol. 9, pp. 36968-36979, 2021.

B. Yadav and S. H. Wadhwani, "An Improved 3DES Encryption Algorithm for Secure Data Transmission in Cloud Computing," in IEEE Access, vol. 9, pp. 17187-17200, 2021.

T. F. Kan, Y. Sun and B. Yan, "A Novel Method of 3DES Encryption with Key Distribution and Verification," in IEEE Access, vol. 9, pp. 81312-81320, 2021.

S. K. Soni and P. S. Chauhan, "A Review on 3DES Encryption Algorithm," in IEEE 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2021, pp. 758-762.

M. A. Rahman, A. B. M. A. Awwal and A. M. A. H. Akhand, "Enhancing Security of 3DES Algorithm by Changing Key Length," in IEEE Access, vol. 9, pp. 89717-89724, 2021.

S. Jiang, G. Zhang, S. Chen and Y. Qiao, "A High-Throughput 3DES Cryptographic Engine with Lightweight Key Schedule," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 5, pp. 1109-1123, May 2021.

R. Jiang, X. Zhang, C. Xiong, Y. Lu and J. Li, "A High-Performance 3DES Encryption Algorithm Based on CUDA," in IEEE Access, vol. 9, pp. 99647-99661, 2021.