PENERAPAN ALGORITMA AES PADA KEAMANAN URL STUDI KASUS *WEBSITE* MAHASISWA ATMA LUHUR

SKRIPSI

Asih Indriati
1911500035

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS ATMA LUHUR
PANGKALPINANG
2023

PENERAPAN ALGORITMA AES PADA KEAMANAN URL STUDI KASUS *WEBSITE* MAHASISWA ATMA LUHUR

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

Asih Indriati

1911500035

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS ATMA LUHUR
PANGKALPINANG

2023

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

NIM	:	1911500035
Nama	:	Asih Indriati
Judul Skripsi	:	PENERAPAN ALGORITMA AES PADA KEAMANAN URL STUDI KASUS *WEBSITE* MAHASISWA ATMA LUHUR

Menyatakan bahwa Laporan Skripsi Saya ini adalah hasil karya sendiri dan bukan plagiat. Apabila tenyata ditemukan di dalam laporan Skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 04 Agustus 2023

Asih Indriati

i

LEMBAR PENGESAHAN SKRIPSI

PENERAPAN ALGORITMA AES PADA KEAMANAN URL STUDI KASUS *WEBSITE* MAHASISWA ATMA LUHUR

Yang dipersiapkan dan disusun oleh

Asih Indriati
1911500035

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 09 Agustus 2023

Susunan Dewan Penguji	**Dosen Pembimbing**
Anggota	
Eza Budi Perkasa, M.Kom	**Yohanes Setiawan Japriadi, M.Kom**
NIDN. 0201089201	**NIDN. 0219068501**
Kaprodi Teknik informatika	**Ketua Penguji**
Chandra Kirana, M.Kom	**Chandra Kirana, M.Kom**
NIDN. 0228108501	**NIDN. 0228108501**

Skripsi ini telah diterima dan sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 11 Agustus 2023

DEKAN FAKULTAS TEKNOLOGI INFORMASI
ISB ATMA LUHUR

Ellya Helmud, M.Kom
NIDN. 0201027901

ii

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang Strata Satu (S1) pada Program Studi Teknik Informatika Fakultas Teknologi Informasi (FTI) Institut Sains dan Bisnis (ISB) Atma Luhur Pangkalpinang.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Bapak dan Ibu tercinta yang telah mendukung penulis.
3. Bapak Drs. Djaetun HS yang telah mendirikan Yayasan Atma Luhur Pangkalpinang.
4. Bapak Prof. Dr. Moedjiono, M.Sc, selaku Rektor ISB Atma Luhur.
5. Bapak Ellya Helmud, M.Kom, selaku Dekan FTI ISB Atma Luhur.
6. Bapak Chandra Kirana, M.Kom, selaku Kaprodi Teknik Informatika.
7. Yohanes Setiawan Japriadi, M.Kom, selaku Dosen Pembimbing.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

Pangkalpinang, 4 Agustus 2023

Penulis

ABSTRACT

AES is an encryption standard with symmetric keys consisting of three block encodings, namely AES-128, AES-192, and AES-256, originally published as Rijndael. The Atma Luhur student website has many pages that are accessed through links to open web pages related to student academic data, for example photos and student academic scores. Each of these pages will form a URL by mentioning the file used, for example https://mahasiswa.atmaluhur.ac.id/ v3/index.php?hal=khs will read the khs.php files, that will be vulnerable to being targeted for attack. This study proposes the use of AES algorithm to encrypt the URL to securing the URL of the Atma Luhur student website. Tests were conducted on 34 URLs of Atma Luhur student websites, resulting in an encryption sukses rate of 100%.

Keywords: AES, cryptography, URL

ABSTRAK

AES merupakan standar enkripsi dengan kunci simetris yang terdiri dari tiga penyandian blok, yaitu AES-128, AES-192, dan AES-256, yang awalnya diterbitkan sebagai Rijndael. *Website* mahasiswa Atma Luhur memiliki banyak halaman yang diakses melalui *link* untuk membuka halaman web yang terkait dengan data akademik mahasiswa, contohnya foto maupun nilai akademik mahasiswa. Masing-masing halaman tersebut akan membentuk suatu URL dengan menyebut file yang digunakan, sebagai contoh https://mahasiswa.atmaluhur.ac.id/v3/index.php?hal=khs akan membaca file khs.php sehingga file tersebut akan rentan menjadi target serangan. Penelitian ini mengusulkan penggunaan algoritma AES untuk mengenkripsi URL yang dimaksud dengan tujuan mengamankan URL *website* mahasiswa Atma Luhur. Pengujian dilakukan terhadap 34 URL *website* mahasiswa Atma Luhur, menghasilkan tingkat keberhasilan enkripsi sebesar 100%.

Kata Kunci: AES, Kriptografi, URL

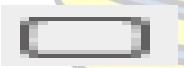
DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

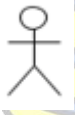
DAFTAR SIMBOL

Simbol *Activity Diagram*

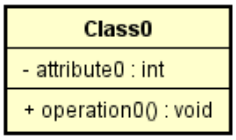
Simbol	Deskripsi
Partisi 	Digunakan untuk mengelompokkan *Action* atau aktivitas berdasarkan individu/objek yang mengeksekusinya. Komponen ini dibentuk dalam notasi *swimlane* secara vertikal.
Initial Node 	Menunjukkan permulaan atau awal aktivitas dari sebuah diagram aktivitas.
Action / Aktivitas 	Menunjukkan aksi atau tindakan yang dilakukan di sistem, aktivitas biasanya diawali dengan kata kerja.
Control Flow / Object Flow 	Menunjukkan arah perpindahan aktivitas atau objek satu ke obyek lainnya.
Decission Node & Merge Node 	Menunjukkan pilihan atau keputusan atau tindakan yang harus diambil pada kondisi tertentu dan penggabungan *node* yang biasanya digunakan untuk percabangan aktivitas jika terdapat lebih dari satu pilihan aktivitas yang dapat dilakukan.
Fork Node 	Menggambarkan pemecahan dari satu aktivitas menjadi dua atau lebih aktivitas yang akan dilakukan secara bersamaan atau paralel.

Join Node 	Menggambarkan penggabungan dua atau lebih aktivitas menjadi satu.
Activity Final 	Menunjukkan akhir atau status akhir yang dilakukan di sistem. Sebuah diagram aktivitas memiliki sebuah status akhir.

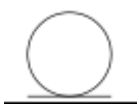
Simbol *Usecase Diagram*

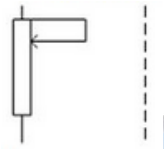
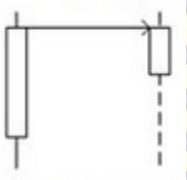
Simbol	Deskripsi
Aktor / *actor* 	Orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.
Usecase 	Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor; biasanya dinyatakan dengan menggunakan kata kerja di awal *frase* nama *Usecase*.
Association	Komunikasi atau interaksi yang dilakukan aktor dengan *usecase*.
include 	Relasi *usecase* tambahan ke sebuah *usecase* di mana *usecase* yang ditambahkan memerlukan *usecase* ini untuk menjalankan fungsinya atau sebagai syarat.

Simbol *Class Diagram*

Simbol	Deskripsi
Class 	Menggambarkan abstraksi dari objek dalam sistem. Kelas digunakan untuk menggambarkan objek-objek dalam sistem yang mempunyai atribut, metode, dan hubungan dengan kelas lain.
Association 	Hubungan antar suatu *class* dengan *class* lainnya. Relasi struktural hubungan antara *class*, menyatakan bahwa objek dari suatu *class* diinstansiasi, digunakan, atau dipanggil oleh objek dari *class* yang lain.

Simbol *Sequence Diagram*

Simbol	Deskripsi
Actor 	Menggambarkan seseorang atau sesuatu (seperti perangkat, sistem lain) yang berinteraksi dengan *boundary*.
Boundary 	Merupakan alat yang digunakan untuk berinteraksi dengan sistem lain, baik berupa *user interface* atau dan lain sebagainya.
Control 	Menggambarkan perilaku untuk mengatur atau kegiatan mengkontrol, mengkoordinasikan perilaku sistem dan dinamika dari suatu sistem, menangani tugas utama, dan mengontrol alur kerja suatu sistem.
Entity 	Menggambarkan informasi yang harus disimpan oleh sistem (struktur data dari sebuah sistem).

Object		Menggambarkan abstraksi dari sebuah entitas nyata/tidak nyata yang informasinya harus disimpan.
Activation		Menunjukkan periode selama suatu obyek atau aktor sedang melakukan suatu tindakan.
Return		Pesan berbalik yang dikirim untuk obyek tertentu.
Object Message		Menggambarkan pesan/hubungan antar obyek yang menunjukkan urutan kejadian yang terjadi.