

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

SKRIPSI



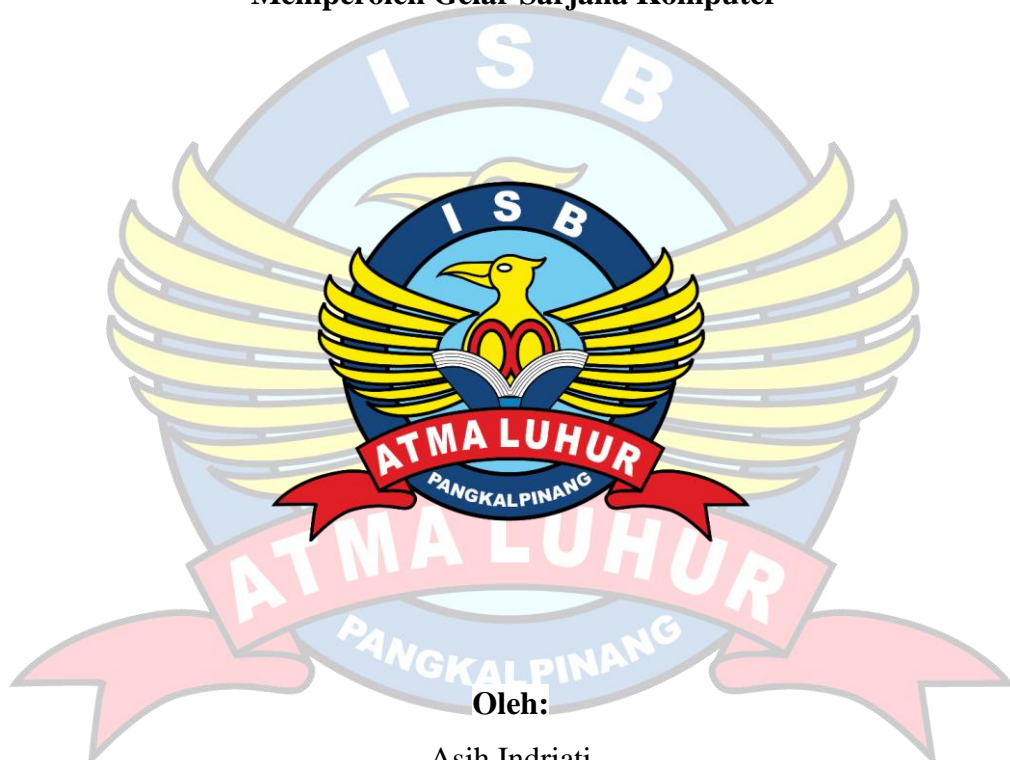
**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS ATMA LUHUR
PANGKALPINANG**

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 ternyata 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



10000
REPUBLIK INDONESIA
10.000
MEPERKAT
TEMPER
C12AKX543031738

Asih Indriati

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
Anggota**


**Eza Budi Perkasa, M.Kom
NIDN. 0201089201**

Dosen Pembimbing


**Yohanes Setiawan Japriadi, M.Kom
NIDN. 0219068501**

Kaprodi Teknik Informatika


**Chandra Kirana, M.Kom
NIDN. 0228108501**

Ketua Penguji


**Chandra Kirana, M.Kom
NIDN. 0228108501**

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

DEKAN FAKULTAS TEKNOLOGI INFORMASI


**Ellya Helmud, M.Kom
NIDN. 0201027901**

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

KATA PENGANTAR	iii
ABSTRACT	iv
ABSTRAK	v
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
DAFTAR SIMBOL	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat Penelitian.....	3
1.5 Sistematika Penulisan	3
BAB II LANDASAN TEORI	5
2.1 Model <i>Iterative</i>	5
2.1.1 Fase dan Tahapan Model <i>Iterative</i>	5
2.1.2 Kelebihan dan Kekurangan <i>Iterative</i>	7
2.2 Definisi Metode Pengembangan Perangkat Lunak.....	8
2.2.1 Metode <i>Object Oriented Programing</i> (OOP)	8
2.2.2 Konsep Dasar <i>Object Oriented Programing</i>	9
2.3 UML (<i>Unified Modelling Language</i>)	10
2.4 Teori Pendukung.....	11
2.4.1 URL	11
2.4.2 Keamanan Data	11
2.4.3 Kriptografi.....	12

2.4.4	Algoritma Kriptografi	14
2.4.5	Jenis Algoritma Kriptografi	15
2.4.6	<i>Advanced Encryption Standard (AES)</i>	16
2.5	Penelitian Terdahulu	22
BAB III METODOLOGI PENELITIAN		24
3.1	Model <i>Iterative</i>	24
3.2	Metode Pengembangan Berorientasi Obyek	24
3.3	UML	24
3.4	Algoritma AES pada Keamanan URL.....	25
BAB IV PEMBAHASAN.....		29
4.1	Tinjauan Organisasi	29
4.1.1	Sejarah ISB Atma Luhur	29
4.1.2	Visi ISB Atma Luhur	29
4.1.3	Misi ISB Atma Luhur	29
4.1.4	Struktur ISB Atma Luhur	31
4.1.5	Tugas dan Wewenang	32
4.2	Analisis Masalah.....	33
4.2.1	Analisa Kebutuhan	33
4.2.2	Analisa Sistem Berjalan	33
4.2.3	Pembahasan Algoritma AES dengan kunci 256 bit	36
4.3	Perancangan Sistem	38
4.3.1	Identifikasi Sistem Usulan	38
4.3.2	Rancangan Sistem	39
4.3.3	Rancangan Layar	55
4.4	Implementasi.....	59

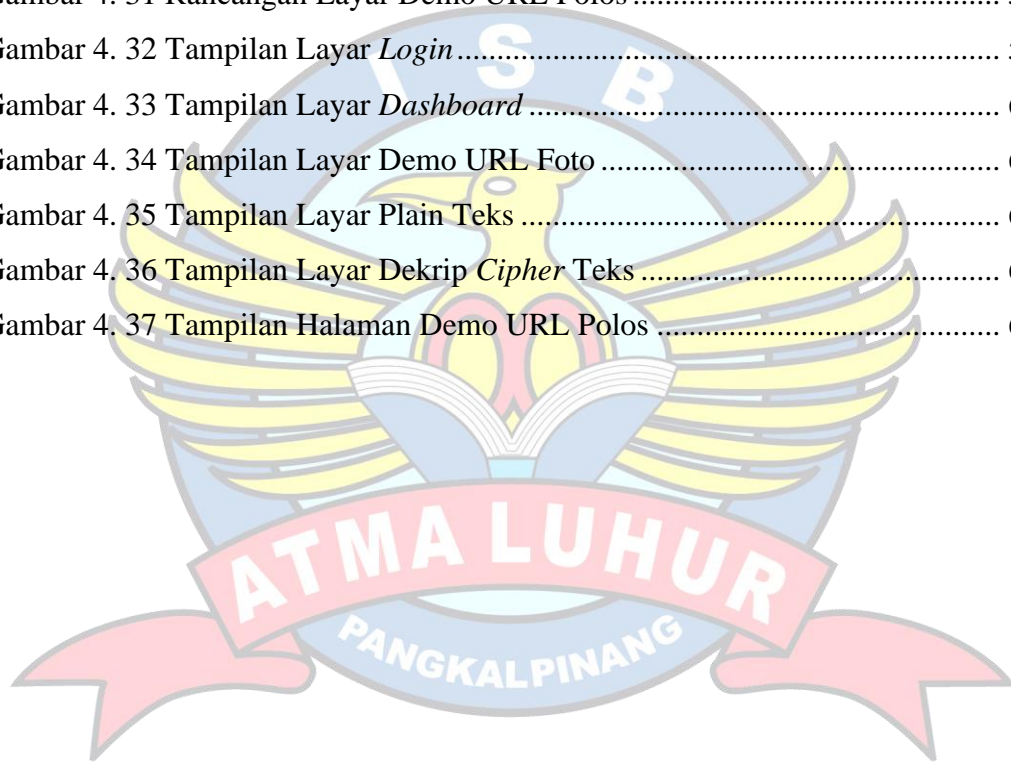
4.4.1 Tampilan Layar	59
4.4.2 Pengujian	63
BAB V PENUTUP.....	68
5.1. Kesimpulan.....	68
5.2. Saran	68
DAFTAR PUSTAKA	69
LAMPIRAN.....	71
Tabel ASCII.....	72
BIODATA PENULIS SKRIPSI.....	77



DAFTAR GAMBAR

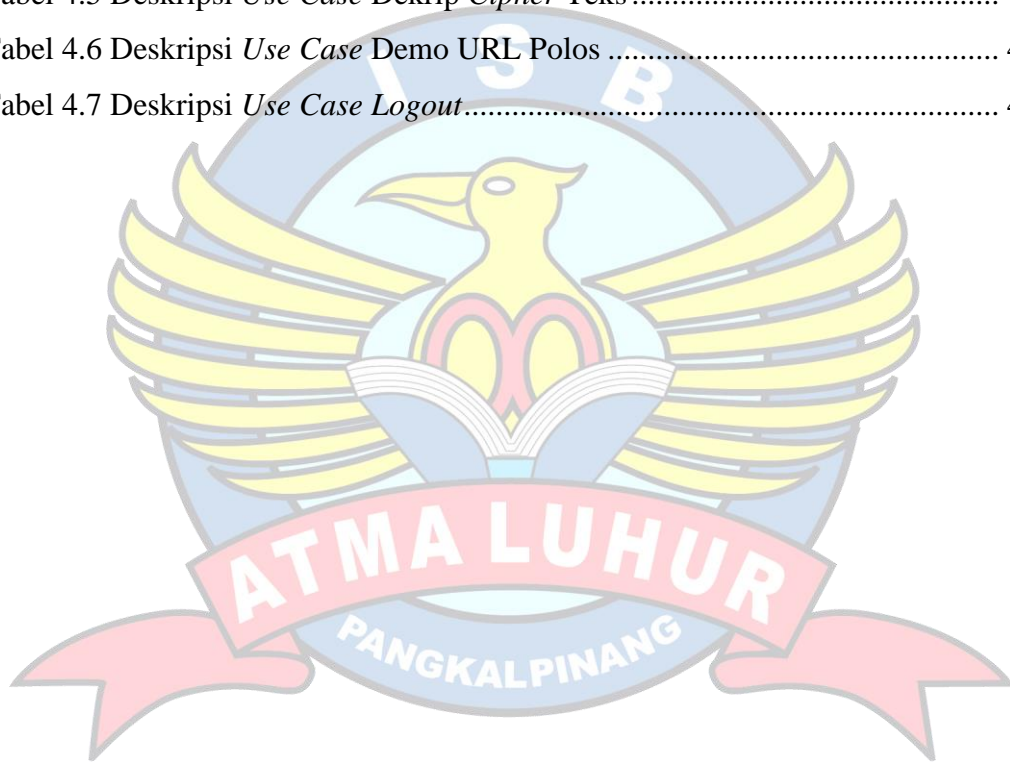
Gambar 2. 1 Model <i>Iterative</i> ^[6]	6
Gambar 2. 2 Algoritma Simetris	15
Gambar 2. 3 Algoritma Asimetris	15
Gambar 2. 4 Proses <i>Input Bytes</i> , <i>State Array</i> , dan <i>Output Bytes</i>	17
Gambar 2. 5 Proses Enkripsi AES ^[13]	18
Gambar 2. 6 Proses Dekripsi AES ^[13]	19
Gambar 2. 7 Tabel <i>S-Box</i> ^[13]	21
Gambar 4. 1 Struktur ISB Atma Luhur	31
Gambar 4. 2 Tampilan Utama <i>Website</i> Mahasiswa Atma Luhur	34
Gambar 4. 3 Tampilan <i>Website</i> Mahasiswa Setelah <i>Login</i>	34
Gambar 4. 4 Pengujian URL Foto Akademik Mahasiswa	35
Gambar 4. 5 Potongan Kode untuk <i>Cipher Key</i>	36
Gambar 4. 6 Fungsi <i>addRoundKey</i>	36
Gambar 4. 7 Fungsi <i>subBytes</i>	37
Gambar 4. 8 Fungsi <i>shiftRows</i>	37
Gambar 4. 9 Fungsi <i>mixColumns</i>	37
Gambar 4. 10 Array <i>rCon</i>	38
Gambar 4. 11 Konversi Cipherteks ke Base64	38
Gambar 4. 12 <i>Use Case Diagram</i>	39
Gambar 4. 13 <i>Activity Diagram Login</i>	43
Gambar 4. 14 <i>Activity Diagram Dashboard</i>	44
Gambar 4. 15 <i>Activity Diagram Demo URL Foto</i>	45
Gambar 4. 16 <i>Activity Diagram Plain Teks</i>	46
Gambar 4. 17 <i>Activity Diagram Dekrip Cipher Tekt</i>	47
Gambar 4. 18 <i>Activity Diagram Demo URL Polos</i>	47
Gambar 4. 19 <i>Sequence Diagram Login</i>	48
Gambar 4. 20 <i>Sequence Diagram Dashboard</i>	49
Gambar 4. 21 <i>Sequence Diagram Demo URL Foto</i>	51
Gambar 4. 22 <i>Sequence Diagram Demo Plain Teks</i>	52

Gambar 4. 23 <i>Sequence Diagram</i> Dekrip <i>Cipher</i> Teks	53
Gambar 4. 24 <i>Sequence Diagram</i> Demo URL Polos.....	54
Gambar 4. 25 <i>Class Diagram</i>	55
Gambar 4. 26 Rancangan Layar Halaman <i>Login</i>	55
Gambar 4. 27 Rancangan Layar Halaman <i>Dashboard</i>	56
Gambar 4. 28 Rancangan Layar Demo URL Foto.....	56
Gambar 4. 29 Rancangan Layar Plain Teks	57
Gambar 4. 30 Rancangan Layar Dekrip <i>Cipher</i> Teks.....	57
Gambar 4. 31 Rancangan Layar Demo URL Polos	58
Gambar 4. 32 Tampilan Layar <i>Login</i>	59
Gambar 4. 33 Tampilan Layar <i>Dashboard</i>	60
Gambar 4. 34 Tampilan Layar Demo URL Foto	60
Gambar 4. 35 Tampilan Layar Plain Teks	61
Gambar 4. 36 Tampilan Layar Dekrip <i>Cipher</i> Teks	62
Gambar 4. 37 Tampilan Halaman Demo URL Polos	62



DAFTAR TABEL

Tabel 2. 1 Perbandingan Jumlah Ronde dan Kunci ^[11]	17
Tabel 2. 2 Tinjauan Penelitian Terdahulu	22
Tabel 4. 1 Deskripsi <i>Use Case</i> Melakukan <i>Login</i>	39
Tabel 4. 2 Deskripsi <i>Use Case</i> Melihat <i>Dashboard</i>	39
Tabel 4. 3 Deskripsi <i>Use Case</i> Demo URL Foto	40
Tabel 4. 4 Deskripsi <i>Use Case</i> Plain Teks	40
Tabel 4.5 Deskripsi <i>Use Case</i> Dekrip <i>Cipher</i> Teks	41
Tabel 4.6 Deskripsi <i>Use Case</i> Demo URL Polos	42
Tabel 4.7 Deskripsi <i>Use Case Logout</i>	42



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.

Decision 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

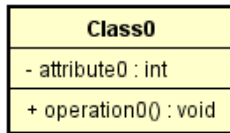


Relasi *usecase* tambahan ke sebuah *usecase* di mana *usecase* yang ditambahkan memerlukan *usecase* ini untuk menjalankan fungsinya atau sebagai syarat.

Simbol *Class Diagram*

Simbol

Class



Deskripsi

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 mengontrol, 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



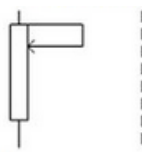
Menggambarkan abstraksi dari sebuah entitas nyata/tidak nyata yang informasinya harus disimpan.

Activation



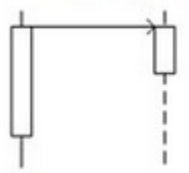
Menunjukkan periode selama suatu obyek atau aktor sedang melakukan suatu tindakan.

Return



Pesan berbalik yang dikirim untuk obyek tertentu.

Object Message



Menggambarkan pesan/hubungan antar obyek yang menunjukkan urutan kejadian yang terjadi.

