

SmileSERV OPEN SOURCE

RSA 암호호화 품 전송

소속: 연길스마일서브소프
트개발유한회사
이름: 한욱

목차



문서 정보	3
이력.....	3
공개.....	3
RSA 암복호화 폼 전송	4
개요.....	4
목적.....	4
RSA란?.....	4
동작 원리.....	5
개요.....	5
다이어그램.....	5
예제 안내.....	6
요구 사항.....	6
폴더 구조.....	6
행 순서.....	7
기타.....	9
오픈 소스.....	9
주요 메소드.....	9

문서 정보

이력

작성일	작성자	비고
2015년 04월 17일	한욱	최초 작성

공개

작성일	공개자	비고
2015년 4월 17일	한욱	최초 공개

RSA 암호화 폼 전송

개요

목적

RSA 암호화 폼 전송은 스마일서브에서 제작한 오픈소스(Open Source)로, HTTP 기반에서 전달되는 POST 혹은 GET 방식의 폼(Form) 데이터를 해커로부터 안전하게 보호하기 위하여 만들어졌습니다.

RSA란?

RSA는 공개키 방식의 암호화 알고리즘으로, 암호화뿐만 아니라 전자서명이 가능한 최초의 알고리즘으로 알려져 있으며, 대표적인 예로 공인인증서가 있습니다.

RSA는 두 개의 키를 사용합니다. 여기서 키란 메시지를 열고(복호화, decrypt) 잠그(암호화, encrypt)는 목적으로 사용되는 상수(constant)를 의미하며, 메시지를 잠그는 목적에 사용되는 키를 공개키(public key)라하고 하며, 메시지를 여는 목적에 사용되는 키를 개인키(private key)라고 합니다.

일반적으로 RSA 알고리즘의 공개키는 공개되어 있으며, 암호화된 메시지는 개인키를 가진 자만이 복호화 할 수 있습니다. 하지만, RSA 알고리즘은 개인키로 암호화하고 공개키로 복호화 할 수도 있습니다. 그러나, 대부분의 RSA 알고리즘을 이용한 어플리케이션은 공개키로 암호화하고 개인키로 복호화하는 일반적인 규칙을 따르고 있습니다.

이와 같은 방식의 암호화 알고리즘을 공개키 알고리즘이라고 하며, 공개된 공개키로 누구나 어떤 메시지를 암호화할 수 있지만, 그것을 해독하여 열람할 수 있는 사람은 개인키를 지닌 사람만이 가능하다는 점에서 대칭키 알고리즘과 차이를 가집니다.

즉, 공개키 알고리즘은 암호화된 메시지를 가로채는 사람이 있어도, 개인키가 없으면 메시지를 열람 할 수 없습니다. 또한, RSA는 소인수 분해의 난해함에 기반하여, 공개키만을 가지고는 개인키를 쉽게 짐작할 수 없도록 디자인되어 있습니다.

RSA 암호화 알고리즘은 1983년에 발명자들이 소속되어 있던 매사추세츠 공과대학교(MIT)에 의해 미국에 특허로 등록되었고, 2000년 9월 21일에 그 특허가 만료되었습니다.

※ 참조: 위키백과, MIT 라이선스

RSA 암호화 폼 전송		작성자	한옥
		작성일	2015년04월17일
부제	SmileSERV OPEN SOURCE	페이지	4 / 9

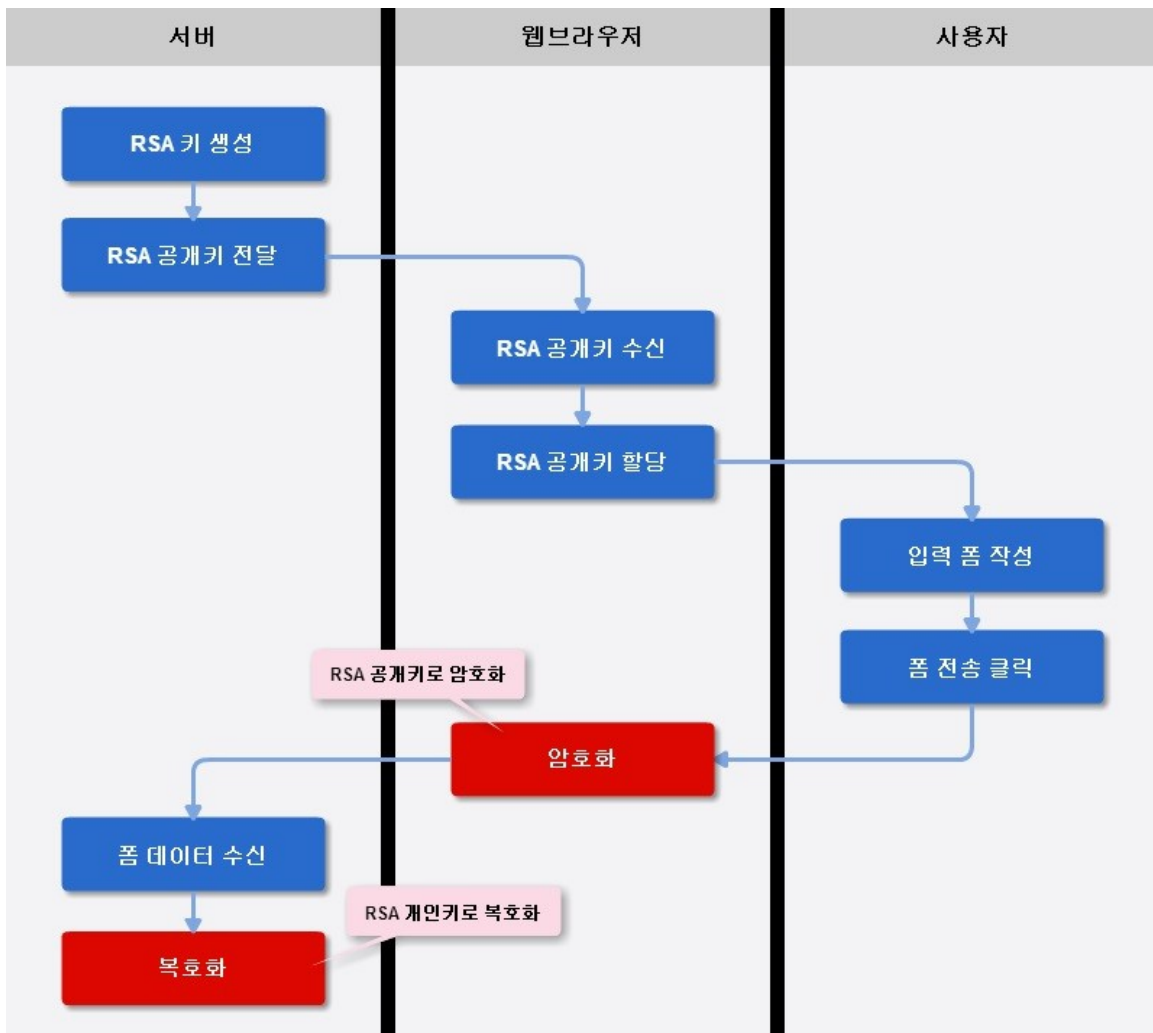
동작 원리

개요

RSA 암호화 폼 전송은 다음과 같은 동작 원리를 가지고 있습니다.

1. 서버 측에서 RSA 키(개인키 및 공개키)를 생성합니다.
2. 폼 전송 전, 사용자가 입력한 내용을 공개키로 암호화합니다.
3. 폼 전송 후, 수신된 폼 데이터를 개인키로 복호화합니다.

다이어그램



RSA 암호화 폼 전송		작성자	한옥
		작성일	2015년04월17일
부제	SmileSERV OPEN SOURCE	페이지	5 / 9

예제 안내

요구 사항

프로그램의 정상적인 구동을 위해서는 다음과 같은 기반 환경이 필요합니다.

구분	버전	비고
웹 서버	x ~ x	Apache Tomcat 등 웹 서비스 구동을 위한 서버 프로그램
JSP, JAVA	1.8.x	1.8.x 이하 버전은 동작될 수 있으나, 테스트되지 않았습니다.

폴더 구조

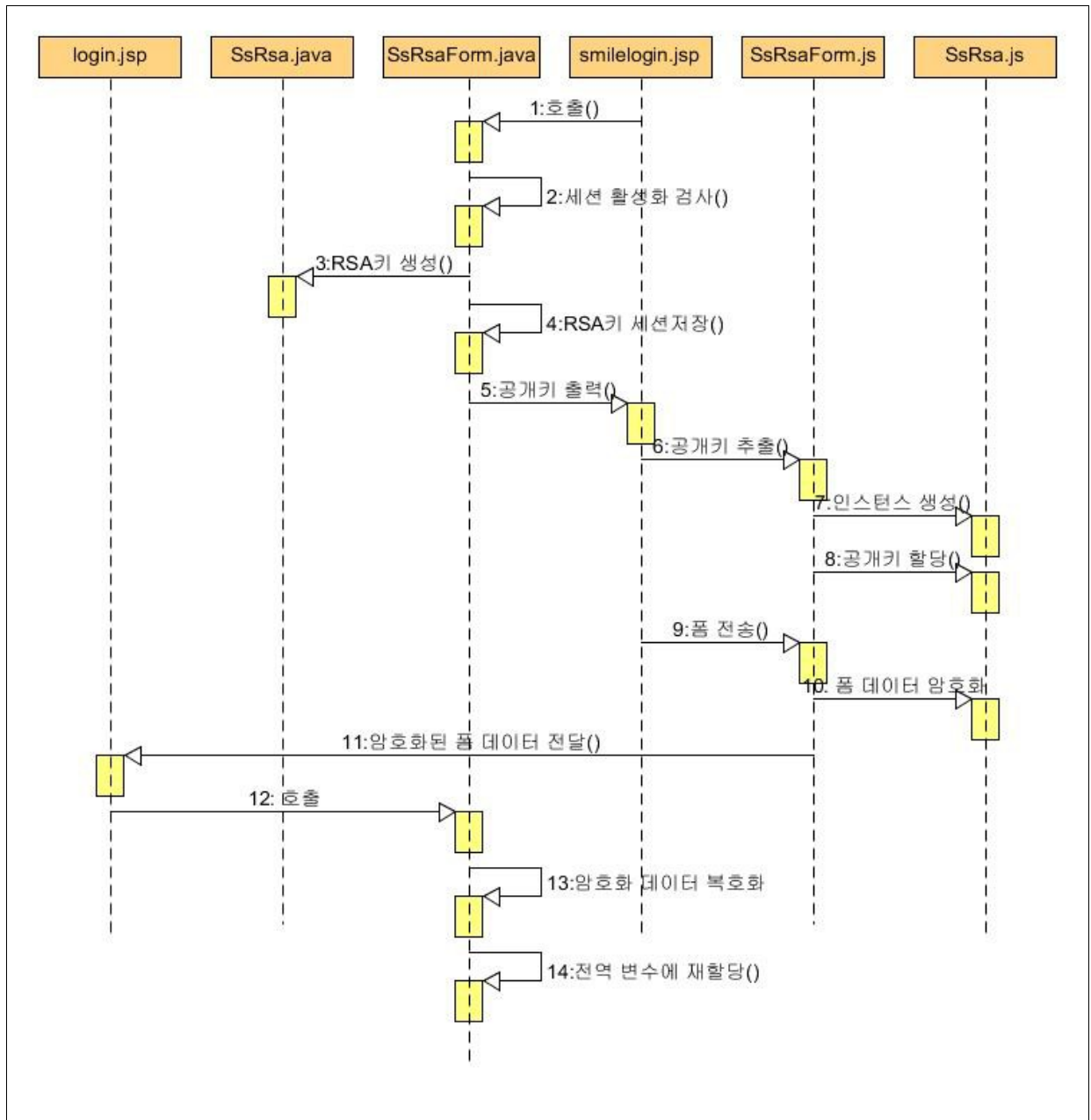
예제로 제공되는 프로그램 소스는 다음과 같은 폴더 구조를 가지고 있습니다. 적색으로 표기된 파일은 프로그램 구동에 반드시 필요한 필수 파일이며, 그 외는 예제 구현을 위하여 생성된 파일입니다.

<ul style="list-style-type: none"> ▶ RSApage <ul style="list-style-type: none"> ▶ Deployment Descriptor: RSApage ▶ JAX-WS Web Services ▶ Java Resources <ul style="list-style-type: none"> ▶ src <ul style="list-style-type: none"> ▶ com.smilesevr.rsa <ul style="list-style-type: none"> ▶ SsRsa.java ▶ SsRsaForm.java ▶ Libraries ▶ JavaScript Resources ▶ build ▶ WebContent <ul style="list-style-type: none"> ▶ css <ul style="list-style-type: none"> reset.css ssKeyboard.css ▶ image <ul style="list-style-type: none"> flow.jpg keyboard.png ▶ META-INF ▶ script <ul style="list-style-type: none"> ssKeyboard.js ssKeyboard.min.js ssRsa.js ssRsa.min.js ssRsaForm.js ▶ WEB-INF <ul style="list-style-type: none"> include_footer.jsp include_header.jsp include_join.jsp include_join2.jsp include_left.jsp include_login.jsp include_login2.jsp join.jsp login.jsp smilejoin.jsp smilelogin.jsp 	<p>// 클래스 파일이 들어있는 폴더입니다.</p> <p>// RSA 알고리즘 코어 클래스입니다.</p> <p>// RSA 암호/복호화 자동 클래스입니다.</p> <p>// 스타일시트(CSS) 파일이 들어있는 폴더입니다.</p> <p>// 스타일시트 초기화를 위한 설정입니다.</p> <p>// 가상 키보드 스타일시트 설정입니다.</p> <p>// 이미지 파일이 들어있는 폴더입니다.</p> <p>// 플러우 차트 설명용 이미지입니다.</p> <p>// 가상 키보드 입력 품용 아이콘입니다.</p> <p>// javascript 파일이 들어있는 들어있는 폴더입니다.</p> <p>// 가상 키보드 코어 스크립트입니다.</p> <p>// 성능 최적화를 위한 소스 압축본입니다.</p> <p>// RSA 알고리즘 코어 클래스입니다.</p> <p>// 성능 최적화를 위한 소스 압축본입니다.</p> <p>// RSA 암호/복호화 자동화 스크립트 입니다.</p> <p>// 웹 페이지의 풋터 영역 HTML 조각입니다.</p> <p>// 웹 페이지의 헤더 영역 HTML 조각입니다.</p> <p>// 웹 페이지의 결과 출력용 HTML 조각입니다.</p> <p>// 웹 페이지의 결과 출력용 HTML 조각입니다.</p> <p>// 웹 페이지의 메뉴 영역 HTML 조각입니다.</p> <p>// 웹 페이지의 결과 출력용 HTML 조각입니다.</p> <p>// 웹 페이지의 결과 출력용 HTML 조각입니다.</p> <p>// 회원가입 샘플의 폼 수신 페이지입니다.</p> <p>// 로그인 샘플의 폼 수신 페이지입니다.</p> <p>// 회원가입 샘플의 폼 작성 페이지입니다.</p> <p>// 로그인 샘플의 폼 작성 페이지입니다.</p>
--	---

행 순서

실행 순서의 이해를 돕기 위하여 프로그램 전반의 실행 로직을 시퀀스 다이어그램으로 표현하였습니다. 아래의 이미지를 참고하여 주십시오.

RSA 암호화 폼 전송		작성자	한욱
		작성일	2015년04월17일
부제	SmileSERV OPEN SOURCE	페이지	7 / 9



RSA 암호화 폼 전송

작성자 한옥

작성일 2015년04월17일

기타

오픈 소스

프로그램 개발에 사용된 오픈 소스는 다음과 같습니다.

구분	버전	URL	참조 대상
jquery	1.8	http://jquery.com	전역에서 사용되는 모든 Javascript

주요 메소드

RSA 암호/복호화에 사용되는 주요 메소드는 다음과 같습니다.

구분	파일명	메소드	비고
JSP	ssRsa.java	makeKey	RSA 키를 생성합니다.
		encrypt	인수로 전달된 문자열을 암호화합니다.
		decrypt	인수로 전달된 문자열을 복호화합니다.
Javascript	ssRsa.js	RSA.setKey	RSA 키를 할당합니다.
		encrypt	인수로 전달된 문자열을 암호화합니다.
		decrypt	인수로 전달된 문자열을 복호화합니다.