SmileSERV OPEN SOURCE

RSA 암복호화 폼 전송

소속: 솔루션개발팀
이름: 고광진

목차

문서 정보

이력

작성일	작성자	비고
2015년 02월 24일	고광진	최초 작성
2015년 04월 16일	고광진	예제에 대한 설명 및 메소드 레퍼런스 추가

공개

작성일	공개자	비고
2015년 2월 24일	고광진	최초 공개

RSA 암복호화 폼 전송

개요

목적

RSA 암복호화 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 수 도 있습니다. 그러나, 대부분의 RSA 알고리즘을 이용한 어플리케이션은 공개키로 암호화하고 개인키로 복호화하는 일반적인 규칙을 따르고 있습니다.

이와 같은 방식의 암호화 알고리즘을 공개키 알로리즘이라고 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 라이센스

동작 원리

개요

RSA 암복호화 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

예제 안내

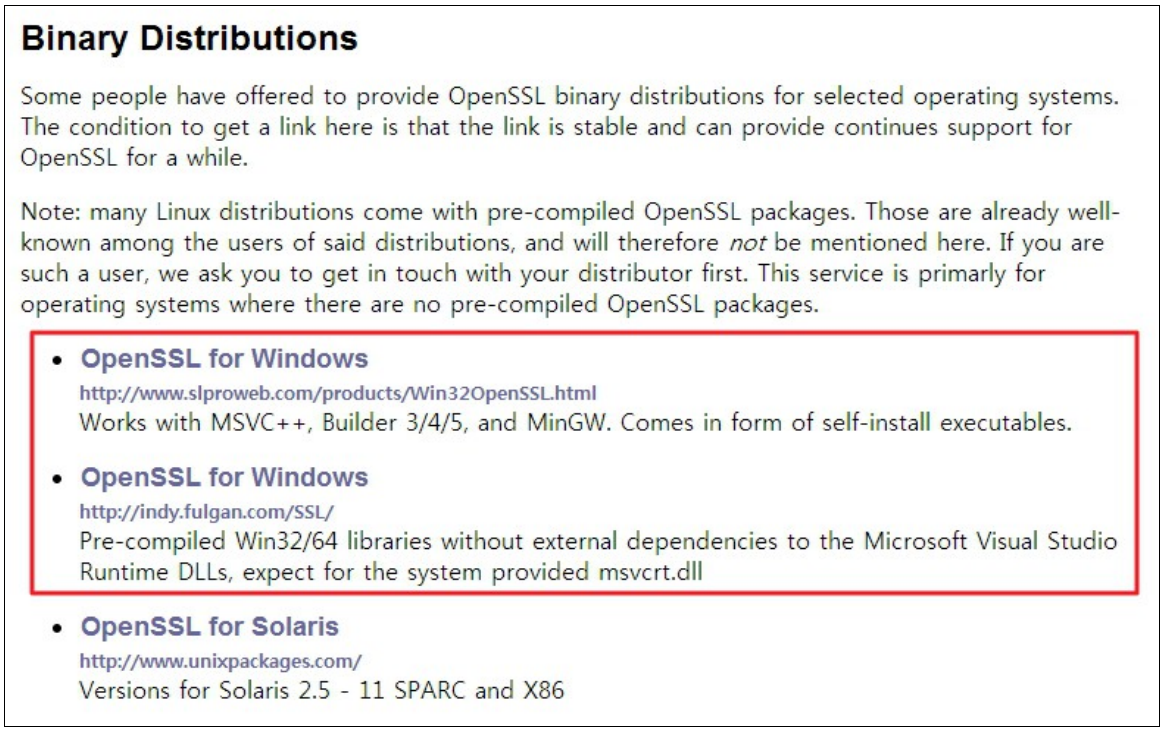
요구 사항

프로그램의 정상적인 구동을 위해서는 다음과 같은 기반 환경이 필요합니다.

구분	버전	비고
웹 서버	x ~ x	Apache 혹은 nginx, IIS 등 웹 서비스 구동을 위한 서버 프로그램
PHP	5.2.x ~ 5.6.x	5.2.x 이하 버전은 동작될 수 있으나, 테스트되지 않았습니다.
OpenSSL	1.x	Linux 기반 시스템은 OpenSSL이 기본으로 설치되어 있습니다.

OpenSSL 라이브러리의 경우, Linux 기반 OS에는 기본으로 설치되어 있습니다만, Windows 기반 OS에는 수동으로 설치를 해야 합니다.

OpenSSL 라이브러리는 무료로 공개된 소스이며, 공식 홈페이지를 통해 다운로드 받을 수 있습니다. 아래의 홈페이지 링크 및 이미지를 참조하여 주십시오.



Binary Distributions

Some people have offered to provide OpenSSL binary distributions for selected operating systems. The condition to get a link here is that the link is stable and can provide continues support for OpenSSL for a while.

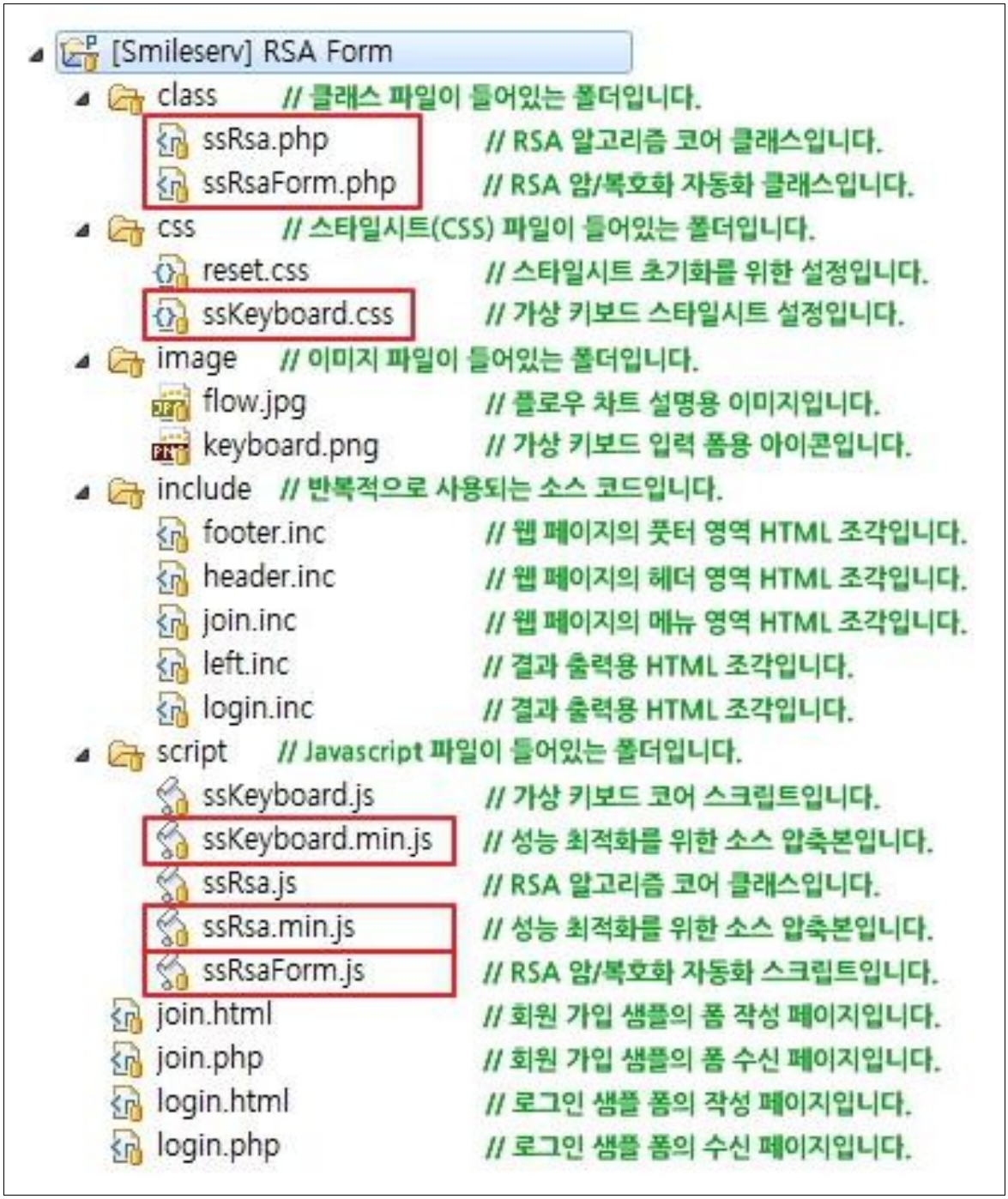
Note: many Linux distributions come with pre-compiled OpenSSL packages. Those are already well-known among the users of said distributions, and will therefore *not* be mentioned here. If you are such a user, we ask you to get in touch with your distributor first. This service is primarly for operating systems where there are no pre-compiled OpenSSL packages.

- **OpenSSL for Windows**
  http://www.slproweb.com/products/Win32OpenSSL.html
  Works with MSVC++, Builder 3/4/5, and MinGW. Comes in form of self-install executables.
- **OpenSSL for Windows**
  http://indy.fulgan.com/SSL/
  Pre-compiled Win32/64 libraries without external dependencies to the Microsoft Visual Studio Runtime DLLs, expect for the system provided msvcrt.dll
- **OpenSSL for Solaris**
  http://www.unixpackages.com/
  Versions for Solaris 2.5 - 11 SPARC and X86

구분	URL	비고
공식 홈페이지	https://www.openssl.org/related/binaries.html	
Win32/64 배포	http://slproweb.com/products/Win32OpenSSL.html	설치형

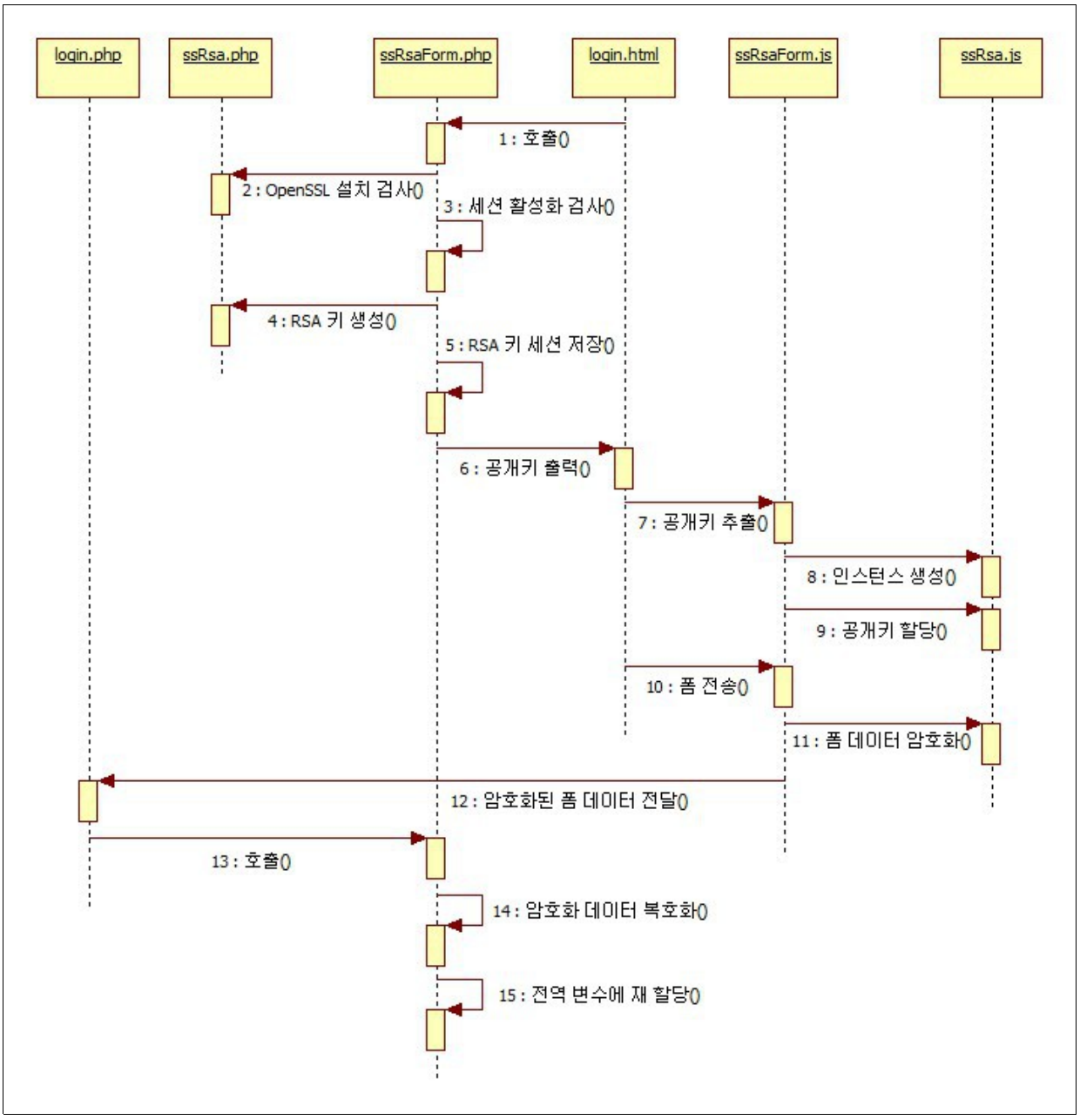
폴더 구조

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.



실행 순서

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



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

phpDoc 주석

RSA 알고리즘 제어 및 자동화 처리를 위하여 생성된 클래스 및 스크립트 파일은 표준화된 주석 규칙(PHP Document)에 의거하여 작성되었습니다.

그러므로, 각 파일의 목적 및 메소드에 대한 사용법은 프로그램의 주석을 참조하여 주십시오. 아래의 URL은 phpDoc에 관련된 홈페이지 및 설명입니다.

구분	URL	비고
phpDocumentor 공식 홈페이지	http://www.phpdoc.org	
phpDoc Tags 안내	http://www.phpdoc.org/docs/latest/index.html	
PHPDoc WiKi 설명	http://en.wikipedia.org/wiki/PHPDoc	

주요 메소드

RSA 암/복호화에 사용되는 주요 메소드는 다음과 같습니다.

구분	파일명	메소드	비고
PHP	ssRsa.php	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.