在 Windows下用 Visual Studio 编译 OpenSSL 1.1.1

到[OpenSSL官方网站](http://www.openssl.org/source/)下载[OpenSSL源代码包](http://www.openssl.org/source/)

1、下载 [openssl-1.1.1.tar.gz](https://www.openssl.org/source/openssl-1.1.0.tar.gz)

2、安装 ActivePerl， 可以到http://www.activestate.com/activeperl/downloads下载最新版本， 需要用到 perl 解释器。

     注：Perl 最低版本要求5.10以上，Windows XP用户最后支持版本ActivePerl 5.20.2.2002 版本

3、使用 VS2010 下的 Visual Studio 2010 Command Prompt 进入控制台模式 (这个模式会自动设置各种环境变量，根据编译32位、64位、Itanium自己选择)。

4、安装dmake，ppm install dmake

5、解压缩 openssl 源代码包，进入 openssl 的根目录， 如 E:\openssl-1.1.0。

6、perl configure VC-WIN32

必须在 c:\openssl-1.1.0 目录下执行该命令， 否则找不到 Configure 文件， 这时就必须指定完整的 Configure 文件路径。

64编译的话 Win64/x64 执行 perl Configure VC-WIN64A；Win64/IA64 执行 perl Configure VC-WIN64I。

7、在正式编译之前

(1). 找到 c:\openssl-1.1.0\configdata.pm和c:\openssl-1.1.0\makefile两个文件， 用记事本打开， 搜索 “/MD” 字符串， 替换成 “/MT”, 这将导致静态链接 C 运行， 避免了在目标机器上安装 VC 再发行包等等操作。

8、编译, nmake

9、编译, nmake test

10、编译, nmake install

      注：openssl 1.1.0开始由原先的libeay32.dll、ssleay32.dll变成了libcrypto-1\_1.dll、libssl-1\_1.dll，一些加密方式也发生了变化。

      比如原先：

      C:\>echo test|openssl enc -base64 -aes-256-cbc -k 123 得到密文：

      U2FsdGVkX19HgMwgeLRw6KIOvhXKrz1keMbCrFuvfh8=

     然后执行C:\>echo U2FsdGVkX19HgMwgeLRw6KIOvhXKrz1keMbCrFuvfh8=|openssl enc -base64 -aes-256-cbc -k 123 -d解密得到原文：

     test

     可是在1.1.0中解密会失败。

1. 生成原始 RSA私钥文件 private\_key.pem

openssl genrsa -out private\_key.pem 1024

2. 将原始 RSA私钥转换为 pkcs8格式

openssl pkcs8 -topk8 -inform PEM -in private\_key.pem -outform PEM -nocrypt -out rsa\_private\_key.pem

3. 生成 RSA公钥 rsa\_public\_key.pem

openssl rsa -in private\_key.pem -pubout -out rsa\_public\_key.crt

4. 从公钥 rsa\_public\_key.pem 获取十六进制的公钥（第一段16进制字符串）

openssl asn1parse -out temp.ans -i -inform PEM<private\_key.pem

最终获取文件列表:

rsa\_private\_key.pem

rsa\_public\_key.crt

16进制公钥字符串用于js端加密