Linux 专栏收录该内容

```c
#include <string.h>
#include <openssl/rsa.h>
#include <openssl/pem.h>
#include <openssl/err.h>
#include <openssl/sha.h>
#include <openssl/crypto.h>

/*
 * 参考https://blog.csdn.net/zjf535214685/article/details/82182241
 */

#define PUBLIC_KEY_PATH  ("./rsapubkey.pem")
#define PRIVATE_KEY_PATH ("./rsaprivatekey.pem")

#define isUseSha256    (1)

#if isUseSha256
#define SHA_WHICH        NID_sha256
#define WHICH_DIGEST_LENGTH    SHA256_DIGEST_LENGTH
#else
#define SHA_WHICH        NID_sha512
#define WHICH_DIGEST_LENGTH    SHA512_DIGEST_LENGTH
#endif


void printHex(unsigned char *md, int len)
{

    int i = 0;
    for (i = 0; i < len; i++)
    {
        printf("%02x", md[i]);
    }

    printf("\n");
}

/*读取私钥*/
RSA* ReadPrivateKey(char* p_KeyPath)
{
    FILE *fp = NULL;
    RSA  *priRsa = NULL;

    printf("PrivateKeyPath[%s] \n", p_KeyPath);

    /*  打开密钥文件 */
    if(NULL == (fp = fopen(p_KeyPath, "r")))
    {
        printf( "fopen[%s] failed \n", p_KeyPath);
        return NULL;
    }
    /*  获取私钥 */
    priRsa = PEM_read_RSAPrivateKey(fp, NULL, NULL,NULL);
    if(NULL == priRsa)
    {
        ERR_print_errors_fp(stdout);
```

分类专栏

0 订阅 19 篇文章 订阅专栏

```
        printf( "PEM_read_RSAPrivateKey\n");
        fclose(fp);
        return NULL;
    }
    fclose(fp);

    return priRsa;
}

/*读取公匙*/
RSA* ReadPublicKey(char* p_KeyPath)
{
    FILE *fp = NULL;
    RSA *pubRsa = NULL;

    printf("PublicKeyPath[%s]\n", p_KeyPath);

    /*  打开密钥文件 */
    if(NULL == (fp = fopen(p_KeyPath, "r")))
    {
        printf( "fopen[%s] \n", p_KeyPath);
        return NULL;
    }
    /*  获取公钥 */
    if(NULL == (pubRsa = PEM_read_RSA_PUBKEY(fp, NULL, NULL,NULL)))
    {
        printf( "PEM_read_RSAPrivateKey error\n");
        fclose(fp);
        return NULL;
    }
    fclose(fp);

    return pubRsa;
}

int test_RSA_sign_verify(void)
{
    char *data = "china";
    char buf[128] = {0};
    RSA *pubKey = NULL;
    RSA *privKey = NULL;
    int nOutLen = sizeof(buf);
    int nRet = 0;

    //1. 对数据进行sha256算法摘要
    unsigned char md[WHICH_DIGEST_LENGTH];
#if isUseSha256
    SHA256((unsigned char *)data, strlen(data), md);
#else
    SHA512((unsigned char *)data, strlen(data), md);
#endif
    printHex(md, WHICH_DIGEST_LENGTH);

    // 2. 读取私钥
    privKey = ReadPrivateKey(PRIVATE_KEY_PATH);
    if (!privKey)
    {
        ERR_print_errors_fp (stderr);
        return -1;
    }

    // 3. 读取公匙
    pubKey = ReadPublicKey(PUBLIC_KEY_PATH);
    if(!pubKey)
    {
        RSA_free(privKey);
        printf("Error: can't load public key");
        return -1;
```

```
    }


    // 4. 签名
    nRet = RSA_sign(SHA_WHICH, md, WHICH_DIGEST_LENGTH, buf, &nOutLen, privKey);
    if(nRet != 1)
    {
        printf("RSA_sign err !!! \n");
        goto quit;
    }
    printf("RSA_sign len = %d:", nOutLen);
    printHex(buf, nOutLen);

    // 5. 验签
    nRet = RSA_verify(SHA_WHICH, md, WHICH_DIGEST_LENGTH, buf, nOutLen, pubKey);
    if(nRet != 1)
    {
        printf("RSA_verify err !!! \n");
        goto quit;
    }
    printf("RSA_verify Success !!! \n");

quit:
    RSA_free(privKey);
    RSA_free(pubKey);

    return 0;
}


int main(int argc, char *argv[])
{
    test_RSA_sign_verify();
    return 0;
}
```

http://www.manongjc.com/detail/15-alqnotqnekvsocu.html

https://www.cnblogs.com/LiuYanYGZ/p/12540577.html

我是谁？？ 关注

1 0 5 专栏目录

我是谁？？

码龄6年 暂无认证

71 原创

2353 积分

私信 关注

Microsoft Visio Pro 2016产品密钥破解完整免费下载 75790

Windows上安装deepin双系统 26589

安卓系统框架介绍 12982

Linux + HyperLPR 进行车牌识别 8381

最新评论

开源人脸识别项目insightface_pytorch
m0_46709917: 我看github上官方提供的有res18等 意思是这些网络也能用吗大佬

Linux + HyperLPR 进行车牌识别
reoreoreoreoreoreo: 那个识别车牌的demo返回的不对啊

基于HyperLPR的车牌识别
zp1501799452: 楼主，安装使用的教程链接失效了，可不可以再发一个啊

ubuntu16.04+cuda10.1安装opencv-3.3.0
我爱人工智能: 写的好，很nice,期待大佬回访！

Windows上CLion配置和使用教程
人生海海，不过尔尔: 跑不起来mingw难死了

您愿意向朋友推荐“博客详情页”吗？

强烈不推荐 不推荐 一般般 推荐 强烈推荐

最新文章

YOLOv5训练自己的数据集(行人检测)

Windows 10 +VS2019 编译OpenCV 4.1.0

Ubuntu + cuda + anaconda + cudatoolkit关系说明

2021年 29篇　2020年 29篇
2019年 90篇　2017年 1篇
2016年 1篇

C++使用openssl建立证书,进行签名,验签,加密,解密(基于... 10-22
意思就是type需要为NID_sha1,NID_md5,等等哈希类型,然后m是信息摘要(坑点),m_len是该摘要的长度,sigbuf是签名的内容,siglen是签名长度(坑点),rsa是…

调用OpenSSL实现数字签名功能例程(一) - Micheal - CSDN博客 11-19
功能:调用OpenSSL实现数字签名功能例程(一) 环境:VS2008+SP1,OpenSSL1.0.1 */ void InitOpenSSL() { ERR_load_crypto_strings(); } unsigned char * …

数字签名算法的实现用c语言,基于openssl的数字签名算法的实现.doc weixin_39832829的博客 63
基于openssl的数字签名算法的实现摘 要随着计算机和互联网技术的不断发展、电子商务的广泛应用，信息安全问题变得越来越重要，而网络信息安全的…

c语言实现用openssl进行数据摘要和签名，sha512 with rsa zjf535214685的博客 3706
因协议要求要在https的消息头里面附带消息体的摘要信息，所以研究了下sha512散列算法和rsa加密算法，下面是用openssl实现的数据sha512算法摘要…

OpenSSL RSA 消息签名与验证 xxh 5498
#include #include #include #include void tSign() { unsigned char sign_value[1024]; //保存签名值的数组 int sign_len; //签名值长度 EVP_MD_CTX mdctx; …

openssl rsa 加密，解密，签名，验签简单例子 热门推荐 yinhua405的博客 1万+
#include #include #include #include #include #include #include #include #include using namespace std; int padding= RSA_PKCS1_PADDING; char pu…

c语言实现rsa签名验证,C语言openssl库RSA签名 weixin_30189603的博客 215
1.源码实现#include #include #include #include #include //公钥验证签名int my_verify(const char *input, int input_len, unsigned char *signret, int signlen,…

使用 OpenSSL 命令行进行 ECC 签名及验签 henter的专栏 4978
首先查看一下 OpenSSL 内建了哪些椭圆曲线，使用命令为： openssl ecparam -list_curves 选择一条椭圆曲线创建 ECC 公私钥对，这里使用 secp256k1…

RSA签名验证示例源码 12-30
基于OpenSSL实现RSA签名与验证流程,使用了RSA_NO_PADDING mode

基于OpenSSL的RSA加解密的C语言实现 01-29
1.该程序是基于OpenSSL的使用纯C语言来实现RSA加解密的，在Linux环境下开发完成，建议在Linux环境下使用（在Windows环境下需要自行修改）； 2…

RSA数字签名程序（C++实现） 06-09
在C++上实现，基于RSA算法，适合新手使用，适合网络安全方面的研究

openssl rsa加密签名 zymx(u010820135)的专栏 3483
from http://blog.csdn.net/cheng0603/article/details/44491983 要使用rsa加密，本来准备在网上找rsa加密算法，但是找到的c源码都不太好用，后来搜索…

C++使用Openssl进行RSA签名(sha1)--完整版 xiaoxianerqq的专栏 6560
转自 ： http://blog.csdn.net/lzyuan1006/article/details/53905575 研究了一天，网上的代码写着是签名，实际上是加密，最开始把我弄得迷糊了，后来慢…

安徽省铜陵市一年级上学期语文期末检测试卷.pdf 10-24
安徽省铜陵市一年级上学期语文期末检测试卷.pdf

宿州市2020年小学英语六年级下学期期末模拟测试卷(2)(I)卷.pdf 最新发布 10-24
宿州市2020年小学英语六年级下学期期末模拟测试卷(2)(I)卷.pdf